

## ALGEBRAIC CURVES WITH MANY AUTOMORPHISMS

MASSIMO GIULIETTI AND GÁBOR KORCHMÁROS

ABSTRACT. Let  $\mathcal{X}$  be a (projective, geometrically irreducible, nonsingular) algebraic curve of genus  $g \geq 2$  defined over an algebraically closed field  $\mathbb{K}$  of odd characteristic  $p$ . Let  $\text{Aut}(\mathcal{X})$  be the group of all automorphisms of  $\mathcal{X}$  which fix  $\mathbb{K}$  element-wise. It is known that if  $|\text{Aut}(\mathcal{X})| \geq 8g^3$  then the  $p$ -rank (equivalently, the Hasse-Witt invariant) of  $\mathcal{X}$  is zero. This raises the problem of determining the (minimum-value) function  $f(g)$  such that whenever  $|\text{Aut}(\mathcal{X})| \geq f(g)$  then  $\mathcal{X}$  has zero  $p$ -rank. For *even*  $g$  we prove that  $f(g) \leq 900g^2$ . The *odd* genus case appears to be much more difficult although, for any genus  $g \geq 2$ , if  $\text{Aut}(\mathcal{X})$  has a solvable subgroup  $G$  such that  $|G| > 126g^2$  then  $\mathcal{X}$  has zero  $p$ -rank and  $G$  fixes a point of  $\mathcal{X}$ . Our proofs use the Hurwitz genus formula and the Deuring Shafarevich formula together with a few deep results from finite group theory characterizing finite simple groups whose Sylow 2-subgroups have a cyclic subgroup of index 2. We also point out some connections with the Abhyankar conjecture and the Katz-Gabber covers.

## 1. INTRODUCTION

Numerous deep results on automorphism groups of algebraic curves, defined over a groundfield of characteristic zero, have been achieved in the passed 125 years following up the seminal work by Hurwitz who was the first to prove that complex curves, other than the rational and elliptic ones, can only have a finite number of automorphisms. Later, Hurwitz's result was given a characteristic-free proof and the fundamental treatment of the theory of automorphisms from the view point of Galois coverings of curves was expanded to include groundfields of positive characteristic. Nevertheless, the theory of automorphism groups of curves present several different features in positive characteristic. This is especially apparent when the curve has many automorphisms, since the classical Hurwitz bound  $|G| \leq 84(g-1)$  on the order of the automorphism group  $\text{Aut}(\mathcal{X})$  of a curve with genus  $g \geq 2$ , fails in positive characteristic whenever  $|G|$  is divisible by the characteristic of the groundfield. As a matter of fact, curves in positive characteristic may happen to have much larger  $\mathbb{K}$ -automorphism group compared to their genus. From previous work by Roquette [37], Stichtenoth [38, 43], Henn [25], and Hansen [22], we know infinite families of curves with  $|\text{Aut}(\mathcal{X})| \approx cg^3$  and it is plausible that there exist many others with  $|\text{Aut}(\mathcal{X})| \approx cg^2$ . Although curves with large automorphism groups may have rather different features, they seem to share a common property, namely their  $p$ -rank is equal to zero. This raises the problem of determining a function  $f(g)$  such that if a curve  $\mathcal{X}$  defined over a field of characteristic  $p > 0$  has an automorphism group  $G$  with  $|G| \geq f(g)$  then  $\mathcal{X}$  has zero  $p$ -rank. A lower bound on  $f(g)$  is  $8g^3$ , as a corollary to Henn's classification [25], see also [26, Theorem 11.127]. Our results stated in Theorems 1.1 and 1.2 show for **odd**  $p$  that if either  $\text{Aut}(\mathcal{X})$  is solvable or  $g$  is even then  $f(g) > cg^2$  for some constant  $c$  independent of  $g$  and  $p$ .

For a subgroup  $G$  of  $\text{Aut}(\mathcal{X})$ , a related question is to determine  $p(G)$  and  $G/p(G)$  where  $p(G)$  is the (normal) subgroup of  $G$  generated by its  $p$ -subgroups. The necessary part of the *Abhyankar Conjecture for affine curves* states that if  $G$  has exactly  $r$  short orbits then the factor group  $G/p(G)$  has a generating set of size at most  $2\bar{g} + r - 1$  where  $\bar{g}$  is the genus of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/G$ . If  $\mathcal{X}/G$  is rational (in particular

---

2010 *Mathematics Subject Classification.* 14H37.

*Key words and phrases.* Algebraic curves, Positive characteristic, Automorphism groups,  $p$ -rank.

The research was supported by Ministry for Education, University and Research of Italy MIUR (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

when  $G$  is large), then  $G = p(G)$  for  $r = 1$ , and  $G/p(G)$  is cyclic for  $r = 2$ . The Abhyankar Conjecture was stated in [1] and proven by Harbater [23]. Recent surveys of this conjecture are found in [35] and [24]. Theorems 1.1 and 1.2 provide a complete description of  $p(G)$  when  $|G| > 900g^2$  and either  $G$  is solvable or  $g$  is even.

For a subgroup  $G$  of  $\text{Aut}(\mathcal{X})$  the associated Galois cover is a Katz-Gabber  $G$ -cover if  $\mathcal{X}|G$  is rational,  $G$  fixes a point  $P \in \mathcal{X}$ , it has at most one more short orbit  $o$  and  $o$  is tame. Such covers are related with the Nottingham groups consisting of power series over a field  $K$  of positive characteristic with substitution as group operation, and are useful to understand how the Nottingham groups can be realized as automorphisms of a curve over  $K$ ; see [6].

**Theorem 1.1.** *Let  $G$  be a solvable automorphism group of an algebraic curve  $\mathcal{X}$  of genus  $g \geq 2$ . If  $|G| > 126g^2$  then  $\mathcal{X}$  has zero  $p$ -rank. Furthermore,  $G$  fixes a point of  $\mathcal{X}$  and  $G = p(G) \rtimes C$  where  $p(G)$  is a Sylow  $p$ -subgroup of  $G$  and  $C$  is a cyclic group. In particular, the cover  $\mathcal{X}|(\mathcal{X}/G)$  is a Katz-Gabber  $G$ -cover.*

**Theorem 1.2.** *Let  $G$  be a nonsolvable automorphism group of an algebraic curve  $\mathcal{X}$  of even genus  $g \geq 2$ . If  $|G| > 900g^2$  then  $\mathcal{X}$  has zero  $p$ -rank, and  $p(G)$  is isomorphic to one of the following linear groups:  $PSL(2, q)$ ,  $q \geq 5$ ,  $PSU(3, q)$ ,  $q \equiv 1 \pmod{4}$ ,  $SL(2, q)$ ,  $q \geq 5$ ,  $SU(3, q)$ ,  $q \equiv 5 \pmod{12}$ , with  $q$  a power of  $p$ .*

Certain quotient curves of the Hermitian and of the GK curves provide examples covering all cases in Theorem 1.2; see Section 9. The possibilities for the structure of  $G$  in Theorem 1.2 are also determined; see Theorem 10.1. In particular,  $G/p(G)$  is a cyclic group according to Abhyankar's conjecture.

From the framework of this paper, it emerges that the automorphism groups of curves with even genus are subject to several constraints which allow to determine their structures completely; see Theorem 6.16. In some sense, this is an unexpected result since each finite group is the automorphism group of some curve defined over  $\mathbb{K}$ .

The ingredients of the proofs are the Hurwitz genus formula and the Deuring Shafarevich formula together with a few deep results from finite group theory characterizing finite simple groups whose Sylow 2-subgroups have a cyclic subgroup of index 2. We also point out that some of our lemmas are related to the Abhyankar conjecture for curves, proved by Harbater, although our proof of Theorem 1.2 is independent of it.

## 2. BACKGROUND AND PRELIMINARY RESULTS

In this paper,  $\text{Aut}(\mathcal{X})$  stands for the automorphism group of a (projective, non-singular, geometrically irreducible, algebraic) curve  $\mathcal{X}$  of genus  $g \geq 2$  defined over an algebraically closed field of odd characteristic  $p$ .

For a subgroup  $G$  of  $\text{Aut}(\mathcal{X})$ , let  $\bar{\mathcal{X}}$  denote a non-singular model of  $\mathbb{K}(\mathcal{X})^G$ , that is, a projective non-singular geometrically irreducible algebraic curve with function field  $\mathbb{K}(\mathcal{X})^G$ , where  $\mathbb{K}(\mathcal{X})^G$  consists of all elements of  $\mathbb{K}(\mathcal{X})$  fixed by every element in  $G$ . Usually,  $\bar{\mathcal{X}}$  is called the quotient curve of  $\mathcal{X}$  by  $G$  and denoted by  $\mathcal{X}/G$ . The field extension  $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$  is Galois of degree  $|G|$ .

Since our approach is mostly group theoretical, we prefer to use notation and terminology from Finite group theory rather than from Function field theory.

Let  $\Phi$  be the cover of  $\mathcal{X} \mapsto \bar{\mathcal{X}}$  where  $\bar{\mathcal{X}} = \mathcal{X}/G$  is a quotient curve of  $\mathcal{X}$  with respect to  $G$ . A point  $P \in \mathcal{X}$  is a ramification point of  $G$  if the stabilizer  $G_P$  of  $P$  in  $G$  is nontrivial; the ramification index  $e_P$  is  $|G_P|$ ; a point  $\bar{Q} \in \bar{\mathcal{X}}$  is a branch point of  $G$  if there is a ramification point  $P \in \mathcal{X}$  such that  $\Phi(P) = \bar{Q}$ ; the ramification (branch) locus of  $G$  is the set of all ramification (branch) points. The  $G$ -orbit of  $P \in \mathcal{X}$  is the subset of  $\mathcal{X}$   $o = \{R \mid R = g(P), g \in G\}$ , and it is *long* if  $|o| = |G|$ , otherwise  $o(P)$  is *short*. For a point  $\bar{Q}$ , the  $G$ -orbit  $o$  lying over  $\bar{Q}$  consists of all points  $P \in \mathcal{X}$  such that  $\Phi(P) = \bar{Q}$ . If  $P \in o$  then  $|o| = |G|/|G_P|$  and hence  $\bar{Q}$  is a branch point if and only if  $o$  is a short  $G$ -orbit. It may be that  $G$  has no short orbits. This is the case if and only if every non-trivial element in  $G$  is fixed-point-free on  $\mathcal{X}$ , that is, the cover  $\Phi$  is unramified. On the other hand,  $G$  has a finite number of short orbits. For a non-negative integer  $i$ , the  $i$ -th

ramification group of  $\mathcal{X}$  at  $P$  is denoted by  $G_P^{(i)}$  (or  $G_i(P)$  as in [39, Chapter IV]) and defined to be

$$G_P^{(i)} = \{g \mid \text{ord}_P(g(t) - t) \geq i + 1, g \in G_P\},$$

where  $t$  is a uniformizing element (local parameter) at  $P$ . Here  $G_P^{(0)} = G_P$ .

Let  $\bar{g}$  be the genus of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/G$ . The Hurwitz genus formula gives the following equation

$$(1) \quad 2\bar{g} - 2 = |G|(2\bar{g} - 2) + \sum_{P \in \mathcal{X}} d_P.$$

where

$$(2) \quad d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1).$$

Let  $\gamma$  be the  $p$ -rank of  $\mathcal{X}$ , and let  $\bar{\gamma}$  be the  $p$ -rank of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/S$ . The Deuring-Shafarevich formula, see [42] or [26, Theorem 11.62], states that

$$(3) \quad \gamma - 1 = |G|(\bar{\gamma} - 1) + \sum_{i=1}^k (|G| - \ell_i)$$

where  $\ell_1, \dots, \ell_k$  are the sizes of the short orbits of  $G$ .

A subgroup of  $\text{Aut}(\mathcal{X})$  is a  $p'$ -group (or a prime to  $p$ ) group if its order is prime to  $p$ . A subgroup  $G$  of  $\text{Aut}(\mathcal{X})$  is *tame* if the 1-point stabilizer of any point in  $G$  is  $p'$ -group. Otherwise,  $G$  is *non-tame* (or *wild*). Obviously, every  $p'$ -subgroup of  $\text{Aut}(\mathcal{X})$  is tame, but the converse is not always true. By a theorem of Stichtenoth, see [26, Theorem 11.56], if  $|G| > 84(\bar{g} - 1)$  then  $G$  is non-tame. Hence  $G$  has a  $p$ -subgroup fixing a point of  $\mathcal{X}$ . An orbit  $o$  of  $G$  is *tame* if  $G_P$  is a  $p'$ -group for  $P \in o$ .

From Group theory, we frequently use Dickson's classification of finite subgroups of the projective linear group  $\text{PGL}(2, \mathbb{K})$ ; see [45] and also [26, Theorem A.8].

**Lemma 2.1.** *Any finite subgroup of the group  $\text{PGL}(2, \mathbb{K})$  is isomorphic to one of the following groups:*

- (i) *prime to  $p$  cyclic groups;*
- (ii) *elementary abelian  $p$ -groups;*
- (iii) *prime to  $p$  dihedral groups;*
- (iv) *the alternating group  $\mathbf{A}_4$ ;*
- (v) *the symmetric group  $\mathbf{S}_4$ ;*
- (vi) *the alternating group  $\mathbf{A}_5$ ;*
- (vii) *the semidirect product of an elementary abelian  $p$ -group of order  $p^h$  by a cyclic group of order  $n > 1$  with  $n \mid (p - 1)$ ;*
- (viii)  $\text{PSL}(2, p^f)$ ;
- (ix)  $\text{PGL}(2, p^f)$ .

### 3. LARGE SOLVABLE AUTOMORPHISM GROUPS OF CURVES

In this section, we prove several lemmas on large solvable automorphism groups of an algebraic curve  $\mathcal{X}$  defined over an algebraically closed field  $\mathbb{K}$  of odd characteristic  $p$ . They together will give a proof for Theorem 1.1.

**Lemma 3.1.** *If  $\mathcal{X}$  has zero  $p$ -rank then  $\text{Aut}(\mathcal{X})$  has the following properties:*

- (i) *a Sylow  $p$ -subgroup of  $\text{Aut}(\mathcal{X})$  fixes a point  $P \in \mathcal{X}$  but its nontrivial elements have no fixed point other than  $P$ ;*
- (ii) *the normalizer of a Sylow  $p$ -subgroup fixes a point of  $\mathcal{X}$ ;*
- (iii) *any two Sylow  $p$ -subgroups have trivial intersection.*

*Proof.* Claim (i) is [26, Theorem 11.129]. Claim (ii) follows from Claim (i). Claim (iii) is [26, Theorem 11.133].  $\square$

**Lemma 3.2.** *Let  $\mathcal{X}$  be an algebraic curve of genus  $g \geq 2$  and  $p$ -rank zero. Let  $G$  be a solvable subgroup of  $\text{Aut}(\mathcal{X})$ . If  $G$  has no nontrivial normal  $p'$ -subgroup then  $G$  fixes a point of  $\mathcal{X}$ .*

*Proof.* Let  $N$  be a minimal normal subgroup of  $G$ . Since  $G$  is solvable,  $N$  is an elementary abelian group. By our hypothesis,  $p \mid |N|$ . Therefore  $N$  is a normal  $p$ -subgroup of  $G$ . Since  $\mathcal{X}$  has zero  $p$ -rank,  $N$  fixes a unique point  $P \in \mathcal{X}$ . Therefore  $G$  fixes  $P$ .  $\square$

**Lemma 3.3.** *Let  $\mathcal{X}$  be an algebraic curve of genus  $g \geq 2$ . Let  $G$  be a solvable subgroup of  $\text{Aut}(\mathcal{X})$  such that  $|G| > 24g^2$ . If  $G$  has some nontrivial normal  $p'$ -subgroup then  $\mathcal{X}$  has zero  $p$ -rank.*

*Proof.* By absurd,  $\mathcal{X}$  is assumed to be a counterexample to the lemma with minimal genus.

Among the normal  $p'$ -subgroups of  $G$  choose one, say  $N$ , of maximal order. We show that the arising quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/N$  has zero  $p$ -rank. This certainly holds if  $\bar{\mathcal{X}}$  is rational. Therefore, two cases are separately investigated according as  $\bar{\mathcal{X}}$  is elliptic or  $g(\bar{\mathcal{X}}) \geq 2$ .

In the former case, take a Sylow  $p$ -subgroup  $S$  of  $G$ . Since the size of  $|G|$  exceeds the Hurwitz bound  $84(g-1)$ , the action of  $G$  has a non-tame orbit on  $\mathcal{X}$ ; then some nontrivial subgroup of  $S$  fixes a point of  $\mathcal{X}$ . Let  $\bar{S} = SN/N$ . Then  $\bar{S}$  is a Sylow  $p$ -subgroup of  $\bar{G} = G/N$ , and some nontrivial subgroup  $\bar{T}$  of  $\bar{S}$  fixes a point of  $\bar{\mathcal{X}}$ . From [26, Theorem 11.94],  $|\bar{T}| = 3$  (and  $p = 3$ ). The Deuring-Shafarevich formula applied to  $\bar{T}$  gives  $\gamma(\bar{\mathcal{X}}) - 1 = 3(\gamma(\bar{\mathcal{Y}}) - 1) + 2\lambda$  where  $\bar{\mathcal{Y}}$  is the quotient curve of  $\bar{\mathcal{X}}$  by  $\bar{T}$  while  $\lambda > 0$  is the number of fixed point of  $\bar{T}$  on  $\bar{\mathcal{X}}$ . Since  $0 \leq \gamma(\bar{\mathcal{Y}}) \leq \gamma(\bar{\mathcal{X}}) \leq g(\bar{\mathcal{X}}) \leq 1$ , this equation implies  $\gamma(\bar{\mathcal{X}}) = 0$ .

In the latter case,  $g(\bar{\mathcal{X}}) \geq 2$  and hence  $g \geq 3$ . From the Hurwitz genus formula applied to  $N$ ,

$$g \geq |N|(g(\bar{\mathcal{X}}) - 1) + 1.$$

Note that  $(|N|(g(\bar{\mathcal{X}}) - 1) + 1)^2 > |N|g(\bar{\mathcal{X}})^2$ . Therefore,

$$|\bar{G}| = \frac{|G|}{|N|} > \frac{24g^2}{|N|} > 24g(\bar{\mathcal{X}})^2.$$

Since  $\mathcal{X}$  is a minimal counterexample, this implies  $\gamma(\bar{\mathcal{X}}) = 0$ .

To prove  $\gamma(\mathcal{X}) = 0$ , observe first that  $\bar{G} = G/N$  is a nontrivial solvable group. Therefore,  $\bar{G}$  has a nontrivial minimal normal subgroup  $\bar{M}$ . Let  $M$  be the normal subgroup of  $G$  such that  $M/N = \bar{M}$ . Then  $M$  contains  $N$  properly, and hence  $p$  divides  $|M|$ . Since  $p \nmid |N|$ , this yields that  $p$  divides  $|\bar{M}|$ , as well. Since  $\bar{M}$  is a minimal normal subgroup, and  $G$  is solvable,  $\bar{M}$  is a normal (elementary abelian)  $p$ -subgroup of  $\bar{G}$ . As  $\gamma(\bar{\mathcal{X}}) = 0$ ,  $\bar{M}$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ .

Let  $\theta$  be the  $N$ -orbit consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $p \nmid |N|$ , we also have  $p \nmid |\theta|$ . Furthermore,  $\bar{M}$  is a normal subgroup of  $\bar{G}$ . Hence  $\bar{P}$  is also fixed by  $\bar{G}$ . Therefore,  $\theta$  is a  $G$ -orbit.

If  $\theta$  consists of just one point, say  $P$ , then  $G = G_P$ , and  $G$  is the semidirect product of the (unique, normal) Sylow  $p$ -subgroup  $S_p$  by a cyclic  $p'$ -subgroup  $H$ ; see [26, Theorem 11.49]. From this,  $24g^2 < |G| = |S_p||H| \leq |S_p|(4g+2)$  by [26, Theorem 11.60] whence

$$|S_p| > \frac{24g^2}{4g+2} > 6 \frac{g^2}{g+1} > 4g.$$

From [26, Theorem 11.78],  $\mathcal{X}$  has zero  $p$ -rank.

We may assume that  $|\theta| \geq 2$ . Choose a point  $P \in \theta$ . Then  $|G| = |G_P||\theta|$  and the stabilizer  $G_P$  of  $P$  in  $G$  is the semidirect product of a Sylow  $p$ -subgroup  $S_p$  of  $G$  by a cyclic group  $H$  of order  $h$  with  $p \nmid h$ . Since  $N$  is a normal subgroup of  $G$ , we have that  $L = NH$  is a subgroup of  $G$  whose order  $|L|$  is equal to  $|H||N|/|H \cap N|$ .

Obviously,  $\theta$  is an  $L$ -orbit, and hence  $|L| = |L_P||\theta|$  with  $H \leq L_P$ . Since  $|G| = |G_P||\theta| = |S_p||H||\theta|$ , the Lagrange theorem yields that

$$\frac{|G|}{|L|} = |S_p| \frac{|H|}{|L_P|}$$

is an integer. As  $|S_p|$  and  $|L_P|$  are coprime, this yields that  $|L_P|$  must divide  $|H|$ . Hence,  $L_P$  cannot contain  $H$  properly. Thus,  $H = L_P$ , and  $|G| = |S_p||L_P||\theta| = |S_p||L|$ .

If  $L$  contains a (cyclic) subgroup  $T$  of index  $d$  that fixes a point, then  $|L| = d|T| \leq d(4g + 2)$  by [26, Theorem 11.60]. For  $d \leq 3$ , this gives  $24g^2 < |G| \leq 12|S_p|(g + \frac{1}{2})$  whence

$$|S_p| > 2 \frac{g^2}{g + \frac{1}{2}} > \frac{p}{p-1}g.$$

From [26, Theorem 11.78],  $\mathcal{X}$  has zero  $p$ -rank. Therefore, we may assume that every subgroup of  $L$  fixing some point has index  $d \geq 4$ .

Now, apply the Hurwitz genus formula to the quotient curve  $\mathcal{Y} = \mathcal{X}/L$  of  $\mathcal{X}$  by  $L$ . If its genus  $g(\mathcal{Y})$  is at least 2, then  $g - 1 \geq |L|$ . If  $g(\mathcal{Y}) \leq 2$  then  $L$  must have at least one short orbit  $\Lambda$ . Let  $Q \in \Lambda$ . If  $\mathcal{Y}$  is elliptic, then  $2g - 2 \geq |\Lambda|(|L_Q| - 1) \geq \frac{1}{2}|L|$  whence  $4(g - 1) \geq |L|$ . If  $\mathcal{Y}$  is rational, then  $\Lambda$  cannot be the unique short orbit of  $L$  on  $\mathcal{X}$ , as  $2g - 2 = -2|L| + |\Lambda|(|L_Q| - 1) = -|L| - \Lambda$  is impossible by  $g(\mathcal{X}) \geq 2$ . Actually, there must be at least two more short orbits, and if  $n_1$  and  $n_2$  are the sizes of two of them, then

$$2g - 2 \geq -2|L| + |L| - |\Lambda| + 2|L| - (n_1 + n_2) = |L| - (|\Lambda| + n_1 + n_2).$$

Since  $d \geq 4$ , each of the sizes  $|\Lambda|, n_1, n_2$  may be assumed to be at most  $\frac{1}{4}|L|$ . Therefore,  $2g - 2 \geq \frac{1}{4}|L|$  whence  $|L| \leq 8g - 8$ .

This shows that  $|L| \leq 8g - 8$  always holds. Now,  $24g^2 < |G| \leq 8|S_p|(g - 1)$  whence

$$|S_p| > 3 \frac{g^2}{g - 1} > \frac{p}{p-1}g.$$

From [26, Theorem 11.78],  $\mathcal{X}$  has zero  $p$ -rank. □

**Lemma 3.4.** *Let  $\mathcal{X}$  be an algebraic curve of genus  $g \geq 2$ . Let  $G$  be a solvable subgroup of  $\text{Aut}(\mathcal{X})$  such that*

$$(4) \quad |G| > cg^2 \text{ with } c = 84 \frac{p}{p-2}.$$

*If  $G$  has no nontrivial normal  $p'$ -subgroup then  $G$  has zero  $p$ -rank.*

*Proof.* Choose a maximal normal  $p$ -subgroup  $N$  of  $G$ . Then  $|N| = p^h$  with  $h \geq t$ , and the factor group  $\bar{G} = G/N$  contains no normal  $p$ -subgroup. If  $\bar{G}$  is trivial then  $G = N$ , that is,  $G$  is a  $p$ -group, and  $\gamma(\mathcal{X}) = 0$  by Nakajima's bound  $|G| < p/(p-2)(g-1)$  for curves of positive  $p$ -rank; see [26, Theorem 11.84]. Therefore  $|\bar{G}| > 1$  is assumed. Since  $\bar{G}$  is solvable, it has a minimal normal subgroup  $\bar{T}$  which is an elementary abelian group of order  $d^j$  with a prime  $d \neq p$ . Let  $T$  be the subgroup of  $G$  containing  $N$  such that  $\bar{T} = T/N$ . Moreover, let  $S$  be a Sylow  $p$ -subgroup of  $G$ . Then  $S \geq N$ . If  $S = N$  then by Schur-Zassenhaus theorem  $G = S \rtimes L$  with a  $p'$ -subgroup  $L$  of  $G$ . Therefore,  $|G| = |S||L| \leq |S|84(g-1)$  whence  $|S| > \frac{p}{p-2} \cdot \frac{g(\mathcal{X})^2}{g(\mathcal{X})-1}$ . Hence  $\mathcal{X}$  has zero  $p$ -rank by Nakajima's bound. Therefore,  $S \supsetneq N$  is assumed. Then  $\bar{S} = S/N$  is a nontrivial  $p$ -subgroup of  $\text{Aut}(\bar{\mathcal{X}})$  where  $\bar{\mathcal{X}} = \mathcal{X}/N$ .

From [26, Theorem 11.116],  $G$  has a unique non-tame short orbit, say  $\theta$ . Since  $N$  is a normal subgroup,  $\theta$  is partitioned into  $N$ -orbits, each of the same length  $p^{h-k}$  where  $p^k = |N_P|$  for any point of  $P \in \theta$ . If  $\lambda$  counts the components of the partition, then  $N$  has exactly  $\lambda$  short orbits and  $|\theta| = \lambda p^{h-k}$ . Observe that if  $\theta$  consists of a single point  $Q$ , then that point is fixed by  $G$ . Since  $|G_Q| > 24g(\mathcal{X})^2$  implies  $\gamma(\mathcal{X}) = 0$ , the case  $|\theta| = 1$  is dismissed.

We show that if  $\lambda = 1$  then  $\gamma(\bar{\mathcal{X}}) \geq 2$ . For  $\lambda = 1$ , the Deuring-Shafarevich formula applied to  $N$  gives  $\gamma(\mathcal{X}) - 1 = p^h(\gamma(\bar{\mathcal{X}}) - 1) + (p^h - p^{h-k})$ . From this  $\gamma(\bar{\mathcal{X}}) - 1 \geq 0$ , otherwise  $\gamma(\mathcal{X}) = 0$ . Furthermore, if

$\gamma(\bar{\mathcal{X}}) = 1$  then  $\gamma(\mathcal{X}) - 1 = p^h - p^{h-k}$ . On the other hand, if  $\mathcal{X}$  has positive  $p$ -rank then Nakajima's bound, see [26, Theorem 11.84], together with  $|S| > |N|$  yield  $\gamma(\mathcal{X}) - 1 \geq \frac{p-2}{p}|S| \geq \frac{p-2}{p}p^{h+1}$ . Therefore,

$$p^h - p^{h-k} \geq \frac{p-2}{p}p^{h+1},$$

a contradiction since  $p > 2$ .

We show that if  $\lambda > 1$  then  $G_P^{(1)} \not\cong N_P$  for every point in  $\theta$ . If  $|N_P| = 1$  this trivially holds, and hence  $k > 0$  is assumed. From the Deuring-Shafarevich formula applied to  $N$ ,  $\gamma(\mathcal{X}) - 1 = p^h(\gamma(\bar{\mathcal{X}}) - 1) + \lambda(p^h - p^{h-k}) \geq -p^h + \lambda(p^h - p^{h-k})$  whence

$$(5) \quad \gamma(\mathcal{X}) - 1 \geq \lambda p^h \left(1 - \frac{1}{\lambda} - \frac{1}{p^k}\right) \geq \lambda p^h \left(1 - \frac{1}{2} - \frac{1}{3}\right) \geq \frac{1}{6}\lambda p^h = \frac{1}{6}p^k|\theta|.$$

For a point  $P \in \theta$ , write  $G_P = G_P^{(1)} \rtimes H$  where  $H$  is a  $p'$ -subgroup of  $G$  fixing  $P$ . Then  $|H| \leq 4g + 2$ , see [26, Theorem 11.60]. Now if  $G_P^{(1)} = N_P$  was true, this would yield  $6(\mathfrak{g}(\mathcal{X}) - 1) \geq 6(\gamma(\mathcal{X}) - 1) \geq |G_P^{(1)}||\theta|$  whence

$$24\mathfrak{g}(\mathcal{X})^2 > 6(4\mathfrak{g}(\mathcal{X}) + 2)(\mathfrak{g}(\mathcal{X}) - 1) \geq |G_P^{(1)}||H||\theta| = |G|,$$

a contradiction. As a consequence, if  $\lambda > 1$  then some nontrivial subgroup of  $\bar{S}$  has a fixed point on  $\bar{\mathcal{X}}$ .

Three cases are investigated separately according to the values of  $\mathfrak{g}(\bar{\mathcal{X}})$ .

If  $\bar{\mathcal{X}}$  is rational, then  $\bar{G}$  is isomorphic to a subgroup of  $PGL(2, \mathbb{K})$  of order divisible by  $p$  which has a normal  $p'$ -subgroup isomorphic to  $\bar{T}$ . From the classification of subgroups of  $PGL(2, \mathbb{K})$ , see [26, Theorem A.8],  $p = 3$  and  $\bar{G} \cong \text{Alt}_4$  or  $\bar{G} \cong \text{Sym}_4$ . Therefore,  $24\mathfrak{g}(\mathcal{X})^2 < |G| \leq 3^h|\bar{G}| \leq 8 \cdot 3^{h+1}$  whence  $|S| \geq 3^{h+1} \geq 3\mathfrak{g}(\mathcal{X})^2 > 3\mathfrak{g}(\mathcal{X})$ . From Nakajima's bound, see [26, Theorem 11.84],  $\mathcal{X}$  has zero  $p$ -rank.

If  $\bar{\mathcal{X}}$  is elliptic then  $\lambda > 1$ . Hence  $\bar{S}$  is a subgroup of  $\bar{\mathcal{X}}$  with a nontrivial subgroup  $\bar{R}$  fixing a point of  $\bar{\mathcal{X}}$ . From [26, Theorem 11.94],  $|\bar{R}| = 3$  (and  $p = 3$ ). The Deuring-Shafarevich formula applied to  $\bar{R}$  gives  $\gamma(\bar{\mathcal{X}}) - 1 = 3(\gamma(\bar{\mathcal{Y}}) - 1) + 2\tau$  where  $\bar{\mathcal{Y}}$  is the quotient curve of  $\bar{\mathcal{X}}$  by  $\bar{R}$  while  $\tau > 0$  is the number of fixed point of  $\bar{R}$  on  $\bar{\mathcal{X}}$ . This equation is only consistent with  $\gamma(\bar{\mathcal{X}}) = 0$  and  $\tau = 1$ . As a consequence,  $\bar{S}$  fixes a unique point  $\bar{P}$ . Also,  $\bar{S} = \bar{R}$  and hence  $|S| = 3|N|$ . Furthermore, the  $N$ -orbit  $\omega$  consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$ , is an  $S$ -orbit. Therefore,  $|S_P|/|N_P| = |S|/|N| = 3$  for  $P \in \omega$ . Write  $G_P = S_P \rtimes H$  with a  $p'$ -subgroup fixing  $P$ . If  $k = 0$  then the action of  $N$  is semiregular and  $\gamma(\bar{\mathcal{X}}) = 0$  gives a contradiction. Therefore  $k > 0$  and (5) holds. From (5),  $18(\gamma(\mathcal{X}) - 1) \geq 3 \cdot 3^k|\theta| = |S_P||\theta|$  whence

$$18(4\mathfrak{g}(\mathcal{X}) + 2)(\mathfrak{g}(\mathcal{X}) - 1) \geq 18(4\mathfrak{g}(\mathcal{X}) + 2)(\gamma(\mathcal{X}) - 1) \geq |S_P||\theta||H| = |G|.$$

But this contradicts our hypothesis  $|G| > c\mathfrak{g}^2$ .

If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ , then arguing as in the proof Lemma 3.3 we have  $|\bar{G}| > c\mathfrak{g}(\bar{\mathcal{X}})^2$ . Since  $\bar{T}$  is a normal  $p'$ -subgroup of  $\bar{G}$ , Lemma 3.3 applies to  $\bar{\mathcal{X}}$ . Therefore,  $\bar{\mathcal{X}}$  has zero  $p$ -rank. From Lemma 3.5 below,  $\bar{G}$  fixes a point  $\bar{P} \in \bar{\mathcal{X}}$ . Hence, the  $N$ -orbit consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$  coincides with  $\theta$ . Then  $\theta$  is also an  $S$ -orbit and  $|\theta| = |N|/|N_P| = |S|/|S_P|$  holds. Write  $G_P = G_P^{(1)} \rtimes H$  with a  $p'$ -subgroup  $H$ . Since  $|H| \leq 4\mathfrak{g}(\mathcal{X}) + 2$  by [26, Theorem 11.60], this yields

$$|G| = |G_P||\theta| \leq |S_P||H| \frac{|S|}{|S_P|} \leq |S|(4\mathfrak{g}(\mathcal{X}) + 2).$$

From this,

$$|S| > \frac{c\mathfrak{g}(\mathcal{X})^2}{4\mathfrak{g}(\mathcal{X}) + 2} > 3\mathfrak{g}(\mathcal{X}).$$

Therefore  $\mathcal{X}$  has zero  $p$ -rank by Nakajima's bound; see [26, Theorem 11.78],  $\square$

**Lemma 3.5.** *Let  $G$  be a solvable automorphism group of an algebraic curve  $\mathcal{X}$  of genus  $\mathfrak{g} \geq 2$  and  $p$ -rank zero such that*

$$(6) \quad |G| > c\mathfrak{g}^2 \text{ with } c = 84\frac{p}{p-1}.$$



If  $G$  has some nontrivial normal  $p'$ -subgroup then  $\mathcal{X}$  fixes a point.

*Proof.* Among the normal  $p'$ -subgroups of  $G$  choose one, say  $N$ , of maximal order. Note that  $N \subsetneq G$  holds and the factor group  $\bar{G} = G/N$  is a non-trivial subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ . We show that  $\bar{G}$  fixes a point of  $\bar{\mathcal{X}}$ . Since  $\bar{G}$  is solvable, a minimal normal subgroup  $\bar{T}$  of  $\bar{G}$  is an elementary abelian group. Let  $T$  be the (normal) subgroup of  $G$  containing  $N$  such that  $\bar{T} = T/N$ . Then  $T$  contains  $N$  strictly. Therefore  $p \mid |T|$  whence  $p \mid |\bar{T}|$ . Hence  $\bar{T}$  is a  $p$ -subgroup of  $\bar{G}$ . Since  $\bar{\mathcal{X}}$  has zero  $p$ -rank,  $\bar{T}$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . Therefore,  $\bar{G}$  fixes  $\bar{P}$ .

Let  $\theta$  be the  $N$ -orbit consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$ . Then  $\theta$  is the unique non-tame  $G$ -orbit of  $\mathcal{X}$ . Since  $p \nmid |N|$  implies  $p \nmid \theta$ , a Sylow  $p$ -subgroup  $S$  must fix a point  $P \in \theta$ , that is  $S = S_P$ . If  $\theta$  consists of just one point, then this point is fixed by  $G$ , and the assertion is proven. We may assume  $|\theta| \geq 2$ .

Furthermore,  $|G| = |G_P||\theta|$  and the stabilizer  $G_P$  of  $P$  in  $G$  is the semidirect product of  $S$  by a cyclic group  $H$  of order  $h$  with  $p \nmid h$ . Since  $N$  is a normal subgroup of  $G$ , we have that  $L = NH$  is a subgroup of  $G$  whose order  $|L|$  is equal to  $|H||N|/|H \cap N|$ . Obviously,  $\theta$  is an  $L$ -orbit, and hence  $|L| = |L_P||\theta|$  with  $H \leq L_P$ . Since  $|G| = |G_P||\theta| = |S||H||\theta|$ , the Lagrange theorem yields that

$$\frac{|G|}{|L|} = |S| \frac{|H|}{|L_P|}$$

is an integer. As  $|S|$  and  $|L_P|$  are coprime, this yields that  $|L_P|$  must divide  $|H|$ . Hence,  $L_P$  cannot contain  $H$  properly. Thus,  $H = L_P$  whence  $|L| = |H||\theta|$ . It turns out that

$$(7) \quad 84 \frac{p}{p-1} \mathfrak{g}(\mathcal{X})^2 < |G| = |G_P||\theta| = |S||H||\theta| = |S||L| < |S|84(\mathfrak{g}(\mathcal{X}) - 1) < 84|S|\mathfrak{g}(\mathcal{X}),$$

whence  $|S| > \frac{p}{p-1} \mathfrak{g}(\mathcal{X})$ . As  $G$  is solvable, [14, Theorem 1.1.] yields that  $G$  fixes a point. Therefore the case  $|\theta| > 1$  is impossible.  $\square$

**Lemma 3.6.** *Let  $G$  be a solvable automorphism group of an algebraic curve  $\mathcal{X}$  of genus  $\mathfrak{g} \geq 2$ . If  $|G| > 84 \frac{p}{p-2} \mathfrak{g}^2$  then the cover  $\mathcal{X}|(\mathcal{X}/G)$  is a Katz-Gabber  $G$ -cover.*

*Proof.* The quotient curve  $\mathcal{X}/G$  is rational. Since  $|G| > 24\mathfrak{g}^2$ , either  $G$  has a unique non-tame short orbit, or it has exactly two short orbits one tame, the other non-tame; see [26, Theorems 11.56, 11.116]. From the above five lemmas,  $\mathcal{X}$  fixes a point  $P \in \mathcal{X}$ , and  $G = S \rtimes C$  with a Sylow  $p$ -subgroup  $S$ . Also,  $\mathcal{X}$  has zero  $p$ -rank. From [26, Lemma 11.129], no nontrivial element in  $S$  fixes a point other than  $P$ . Therefore, if  $G$  has a short orbit distinct from  $\{P\}$  then it is tame and unique, and the cover  $\mathcal{X}|(\mathcal{X}/G)$  is a Katz-Gabber  $G$ -cover.  $\square$

#### 4. AUTOMORPHISM GROUPS AND $p$ -RANK

In some cases, the above upper bounds can be improved.

**Lemma 4.1.** *Let  $H$  be a solvable automorphism group of an algebraic curve of genus  $\mathfrak{g} \geq 2$  containing a normal  $d$ -subgroup  $Q$  of odd order such that  $|Q|$  and  $[H : Q]$  are coprime. Suppose that a complement  $U$  of  $Q$  in  $H$  is abelian, and that  $N_H(U) \cap Q = \{1\}$ . If*

$$(8) \quad |H| = c(\mathfrak{g} - 1) \text{ with } c \geq 30,$$

*then  $d = p$  and  $U$  is cyclic. Moreover, the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/Q$  is rational and either*

- (i)  $\mathcal{X}$  has positive  $p$ -rank,  $Q$  has exactly two (non-tame) short orbits, and they are also the only short orbits of  $H$ ; or
- (ii)  $\mathcal{X}$  has zero  $p$ -rank and  $H$  fixes a point.

*Proof.* We have  $H = Q \rtimes U$ . Set  $|Q| = d^k$ ,  $|U| = u$ . Then  $u \neq d$ .

If  $u = 2$  then (8) reads  $|Q| > 15(\mathfrak{g} - 1)$ . If  $d = p$  then  $\mathcal{X}$  has zero  $p$ -rank by Nakajima's bound [32], see also [26, Theorem 11.84]. Otherwise,  $Q$  is a prime to  $p$  subgroup of  $H$ . The Hurwitz genus formula applied

to  $Q$  gives  $|Q| < 6(\mathfrak{g}(\mathcal{X}) - 1)$  for  $d \neq 3$  and  $|Q| < 12(\mathfrak{g}(\mathcal{X}) - 1)$  for  $d = 3$ , contradicting (8). Therefore  $u \geq 3$ .

Three cases are treated separately according as the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/Q$  has genus  $\bar{\mathfrak{g}}$  at least 2, or  $\bar{\mathcal{X}}$  is elliptic, or rational.

If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ , then  $\text{Aut}(\bar{\mathcal{X}})$  has a subgroup isomorphic to  $U$ , and [26, Theorem 11.79] yields  $4\mathfrak{g}(\bar{\mathcal{X}}) + 4 \geq |U|$ . Furthermore, from the Hurwitz genus formula applied to  $Q$ ,  $\mathfrak{g} - 1 \geq |Q|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ . Therefore,

$$(4\mathfrak{g}(\bar{\mathcal{X}}) + 4)|Q| \geq |U||Q| = |H| > c(\mathfrak{g} - 1) \geq c|Q|(\mathfrak{g}(\bar{\mathcal{X}}) - 1),$$

whence

$$c < 4 \frac{\mathfrak{g}(\bar{\mathcal{X}}) + 1}{\mathfrak{g}(\bar{\mathcal{X}}) - 1} \leq 12$$

contradicting (8).

If  $\bar{\mathcal{X}}$  is elliptic, then the cover  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies, otherwise  $\mathcal{X}$  itself would be elliptic. Thus,  $Q$  has some short orbits. Take one of them together with its images  $o_1, \dots, o_u$  under the action of  $H$ . Since  $Q$  is a normal subgroup of  $H$ ,  $o = o_1 \cup \dots \cup o_m$  is a  $H$ -orbit of size  $u_1 d^v$  where  $d^v = |o_1| = \dots |o_m|$ . Equivalently, the stabilizer of a point  $P \in o$  has order  $d^{k-m}u/u_1$ , and it is the semidirect product  $Q_1 \rtimes U_1$  where  $|Q_1| = d^{k-v}$  and  $|U_1| = u/u_1$  for a subgroup  $Q_1$  of  $Q$  and  $U_1$  of  $U$  respectively. The point  $\bar{P}$  lying under  $P$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$  is fixed by the factor group  $\bar{U}_1 = U_1 Q/Q$ . Since  $\bar{\mathcal{X}}$  is elliptic, [26, Theorem 11.94] implies  $|\bar{U}_1| \leq 12$  for  $p = 3$  and  $|\bar{U}_1| \leq 6$  for  $p > 3$ . As  $\bar{U}_1 \cong U_1$ , this yields the same bound for  $|U_1|$ , that is,  $u \leq 12u_1$  for  $p = 3$  and  $u \leq 6u_1$  for  $p > 3$ . Furthermore, if  $p = 3$  then  $d > 3$ , and  $d_P \geq d^{k-m} - 1 \geq \frac{4}{5}d^{k-m}$ . If  $p > 3$  then  $d_P \geq d^{k-m} - 1 \geq \frac{2}{3}d^{k-m}$ . From the Hurwitz genus formula applied to  $Q$ , if  $p = 3$  then

$$2\mathfrak{g} - 2 \geq d^m u_1 d_P \geq d^m u_1 \left(\frac{4}{5}d^{k-m}\right) \geq \frac{4}{5}d^m u_1 \geq \frac{1}{15}d^m u = \frac{1}{15}|Q||U| = \frac{1}{15}|H|,$$

while for  $p > 3$ ,

$$2\mathfrak{g} - 2 \geq d^m u_1 d_P \geq d^m u_1 \left(\frac{2}{3}d^{k-m}\right) \geq \frac{2}{3}d^m u_1 \geq \frac{1}{9}d^m u = \frac{1}{9}|Q||U| = \frac{1}{9}|H|,$$

But this contradicts (8).

If  $\bar{\mathcal{X}}$  is rational, then  $Q$  has at least one short orbit. Furthermore,  $\bar{U} = UQ/Q$  is isomorphic to a subgroup of  $PGL(2, \mathbb{K}) \cong \text{Aut}(\bar{\mathcal{X}})$ . Since  $U \cong \bar{U}$ , Lemma 2.1 shows that either

- (I)  $U$  is an elementary abelian  $p$ -group and  $\bar{U}$  fixes a point  $\bar{P}_\infty$  but no non-trivial element of  $\bar{U}$  fixes a point other than  $\bar{P}_\infty$ , or
- (II)  $U$  is a cyclic group of order prime to  $p$ ,  $\bar{U}$  fixes two points  $\bar{P}_0$  and  $\bar{P}_\infty$  but no non-trivial element in  $\bar{U}$  fixes a point other than  $\bar{P}_0$  and  $\bar{P}_\infty$ .

Let  $o_\infty$  and  $o_0$  be the  $Q$ -orbits lying over  $\bar{P}_0$  and  $\bar{P}_\infty$ , respectively. Obviously,  $o_\infty$  (and in case (II) also  $o_0$ ) is a short orbit of  $H$ . We show that  $Q$  has at most one or two short orbits according to cases (I) and (II), the candidates being  $o_\infty$  and in case (II) also  $o_0$ . By absurd, there is a  $Q$ -orbit  $o$  of size  $d^m$  with  $m < k$  which lies over a point  $\bar{P} \in \bar{\mathcal{X}}$  different from  $\bar{P}_\infty$  (in case (II) from both  $\bar{P}_0$  and  $\bar{P}_\infty$ ). Since the orbit of  $\bar{P}$  in  $\bar{U}$  has length  $u$ , then the  $H$ -orbit of a point  $P \in o$  has length  $ud^m$ . If  $u > 3$ , the Hurwitz genus applied to  $Q$  gives

$$2\mathfrak{g} - 2 \geq -2d^k + ud^m(d^{k-m} - 1) \geq -2d^k + ud^m \frac{2}{3}d^{k-m} \geq -2d^k + \frac{2}{3}ud^k \geq \frac{2}{3}(u - 3)d^k > \frac{1}{6}ud^k \geq \frac{1}{6}|H|,$$

a contradiction with  $|H| > c\mathfrak{g}$  for  $c = 36$ . If  $u = 3$  then  $d \geq 3$ , and hence

$$2\mathfrak{g} - 2 \geq -2d^k + 3d^m(d^{k-m} - 1) = d^k - 3d^m > \frac{1}{3}d^k,$$

whence  $|H| = 3d^k < 9\mathfrak{g}$ , a contradiction with (8).

In case (I),  $u$  is a power of  $p$  with  $p \neq d$  while  $|o_\infty| = d^k$ . Hence  $U$  must fix a point  $P_\infty \in o_\infty$ . As  $o_\infty$  is a short  $Q$ -orbit,  $H_P$  contains a non-trivial element  $v$  from  $Q$ . From [26, Theorem 11.74],  $U$  is a normal subgroup of  $H_P$ . Therefore,  $w \in N_H(U) \cap Q$ , a contradiction.



We are left with case (II). Since  $H$  has exactly two short orbits, (8) together with [26, Theorem 11.56] yield that  $p$ -divides  $|H|$ . Therefore,  $d = p$ . Assume that  $Q$  has two short orbits. They are  $o_\infty$  and  $o_0$ . If their lengths are  $p^a$  and  $p^b$  with  $a, b < k$ , the Deuring-Shafarevich formula applied to  $Q$  gives

$$\gamma(\mathcal{X}) - 1 = -p^k + (p^k - p^a) + p^k - p^b$$

whence  $\gamma(\mathcal{X}) = p^k - (p^a + p^b) + 1 > 0$ . The same argument shows that if  $Q$  has just one short orbit, then  $\gamma(\mathcal{X}) = 0$  and the short orbit consists of a single point  $P$ . Since  $Q$  is a normal subgroup of  $H$ ,  $P$  is also fixed by  $H$ .  $\square$

**Remark 4.2.** Both cases (i) and (ii) in Lemma 4.1 occur as the following examples show. For case (i), let  $\mathcal{X}$  be a non-singular model  $\mathcal{X}$  of the Artin-Mumford curve where  $\mathcal{C}$  is the plane irreducible (singular) curve  $\mathcal{C}$  of affine equation  $(X^p - X)(Y^p - Y) - 1 = 0$ . The main properties of  $\mathcal{X}$  are well known; see [12, 5]:  $\mathcal{X}$  is an ordinary curve  $\mathcal{X}$  of genus  $\mathfrak{g}$  (and  $p$ -rank) equal to  $(p-1)^2$ . Furthermore,  $\mathcal{C}$  has two (ordinary) singular points  $X_\infty$  and  $Y_\infty$  both  $p$ -fold points. Each of them is the center of  $p$  places of  $\mathbb{K}(\mathcal{X})$ . Let  $o_\infty$  be the set of the  $p$  points of  $\mathcal{X}$  associated to the  $p$  places centered at  $X_\infty$ , and  $o_0$  that arising from  $Y_\infty$  in the same way. For every  $a, b \in \mathbb{F}_p$ , the linear map  $(X, Y) \rightarrow (X + a, Y + b)$  is an automorphism of  $\mathcal{C}$  and hence of  $\mathcal{X}$ . The linear maps form an (elementary abelian) group  $Q = C_p \times C_p$  of order  $p^2$ , and  $Q$  has two (short) orbits of length  $p$ , namely  $o_\infty$  and  $o_0$ . Also, for every  $c \in \mathbb{F}_p^*$  the linear map  $(X, Y) \rightarrow (cX, c^{-1}Y)$  is an automorphism of  $\mathcal{C}$  and hence of  $\mathcal{X}$ . They form a cyclic group  $C_{p-1}$  of order  $p-1$  that preserves both  $o_\infty$  and  $o_0$ . A further (linear) automorphism is  $\varphi : (X, Y) \rightarrow (Y, X)$  which interchanges  $o_\infty$  and  $o_0$ . The group generated by  $C_{p-1}$  together with  $\varphi$  is a dihedral group  $D_{p-1}$ . Therefore,  $\text{Aut}(\mathcal{X})$  has a subgroup  $G = (C_p \times C_p) \rtimes D_{p-1}$  with a dihedral group of order  $2(p-1)$ . If  $\mathbb{K} = \overline{\mathbb{F}_p}$  or  $(\mathbb{K}, |\cdot|)$  is non-Archimedean valued field of characteristic  $p$ , then  $\text{Aut}(\mathcal{X}) = G$ ; see [5] and [12]. For  $p \geq 27$ ,  $|H| = p^2(p-1) \geq 30(\mathfrak{g}-1)$  and  $H = (C_p \times C_p) \rtimes C_{p-1}$  satisfies the hypotheses of Lemma 4.1, and we have case (i). For case (ii), let  $\mathcal{X}$  be a non-singular model  $\mathcal{X}$  of the the plane irreducible (singular) curve  $\mathcal{C}$  of affine equation  $Y^p + Y - X^m = 0$  with  $m < p$ . For the main properties of  $\mathcal{X}$ ; see [43], and [26, Theorem 11.56]:  $\mathcal{X}$  has genus  $\frac{1}{2}(p-1)m$  and  $p$ -rank zero while  $H = \text{Aut}(\mathcal{X})$  fixes the infinite point and  $H = S \rtimes C$  with  $|S| = p$  and  $|C| = m(p-1)$ . If  $p \geq 17$  then  $|H| > 30(\mathfrak{g}-1)$ , and we have case (ii).

**Remark 4.3.** In Lemma 4.1, if we assume  $d = p$  then the extra-hypothesis  $N_H(U) \cap Q = \{1\}$  can actually be dropped. In fact, in the proof of Lemma 4.1, the hypothesis  $N_H(U) \cap Q = \{1\}$  is only used to rule out case (I). Obviously, if  $Q$  is a  $p$ -subgroup then  $U$  is a  $p'$ -subgroup, and (I) cannot occur. Furthermore, Lemma 4.1 applies whenever  $H$  is taken for the stabilizer of a point of  $\mathcal{X}$  satisfying (8).

**Remark 4.4.** In Lemma 4.1, if we assume  $d \neq p$  and  $[H : Q] \geq 3$  but drop the extra-hypothesis  $N_H(U) \cap Q = \{1\}$  then case (I) in the proof of Lemma 4.1 occurs. Then  $H$  has a unique short orbit  $o_\infty$  and the quotient curve  $\tilde{\mathcal{X}} = X/H$  is rational. From the Abhyankar conjecture as stated in Section 2,  $H$  is generated by  $U$  together with its conjugates in  $H$ . In particular,  $H$  is not a direct product of  $Q$  and  $U$ . We do not use this fact in the forthcoming proofs.

**Lemma 4.5.** *Let  $T$  be a subgroup of  $\text{Aut}(\mathcal{X})$  containing a normal subgroup  $H$  that satisfies the hypotheses of Lemma 4.1. Then  $T = Q \rtimes V$  where  $V$  is a cyclic or a dihedral group, and  $p$  is prime to  $|V|$ . If, in addition,  $\mathcal{X}$  has positive  $p$ -rank and  $T$  fuses two short  $H$ -orbits together one orbit then  $V$  is dihedral.*

*Proof.* We may suppose that (II) in the proof of Lemma 4.1 holds. Since  $H$  is a normal subgroup of  $T$ , and  $o_\infty$  and  $o_0$  are the only short orbits of  $H$ , two possibilities arise, namely either  $T$  preserves both  $o_\infty$  and  $o_0$ , or  $o_\infty \cup o_0$  is a  $T$ -orbit. On the other hand, as  $[H : Q]$  is prime to  $Q$  and  $Q$  is a normal subgroup of  $H$ ,  $Q$  is the unique Sylow  $p$ -subgroup of  $H$ . Thus  $Q$  is a characteristic subgroup of  $H$ , and hence  $Q$  is a normal subgroup of  $T$ . Therefore,  $\bar{T} = T/Q$  is a subgroup of  $PGL(2, \mathbb{K})$ . It turns out that either  $\bar{T}$  fixes both points  $\bar{P}_0$  and  $\bar{P}_\infty$ , or  $\bar{T}$  interchanges them. From Lemma 2.1,  $\bar{T}$  is cyclic in the former case, and it is a dihedral group in the latter case. In both cases  $p$  is prime to  $|\bar{T}|$ . Therefore  $Q$  is prime to  $[T : Q]$ , and hence  $T = Q \rtimes V$  where  $V$  is either cyclic or dihedral, and  $p$  is prime to  $|V|$ .  $\square$

**Remark 4.6.** In the dihedral case, some (involutory) elements of  $\bar{T}$  fixes a point  $\bar{P}$  distinct from  $P_\infty$  and  $P_0$ . This agrees with the Abhyankar Conjecture as stated in Section 2 which shows that the possibility for  $T$  to be dihedral in Lemma 4.5 can only occur when  $T$  has a short orbit other than the fused one. This is the case when  $\mathcal{X}$  is a no-singular model of the Artin-Mumford curve; see Remark 4.2. In fact, the automorphism  $\varphi : (X, Y) \rightarrow (Y, X)$  of  $\mathcal{C}$  fixes each point  $P(a, a) \in \mathcal{C}$  with  $a^p - a \pm 1 = 0$  and these points are outside  $o_\infty$  and  $o_0$ . We do not use this fact in the forthcoming proofs.

**Lemma 4.7.** *Let  $G$  be an automorphism group of  $\mathcal{X}$  with  $|G| \geq 16g^2$  which has property (iii) of Lemma 3.1. If  $G$  has a Sylow  $d$ -subgroup such that the normalizer  $N_G(Q)$  satisfies the hypotheses on  $H$  in Lemma 4.1 then  $\mathcal{X}$  has zero  $p$ -rank.*

*Proof.* We have  $d = p$ . By absurd, case (II) in the proof of Lemma 4.1 occurs. Therefore, we have exactly two short  $Q$ -orbits  $o_\infty$  and  $o_0$ , and each is left invariant by  $N_G(Q)$ , as well. If they were in two different orbits of  $G$  then case (b) in [26, Theorem 11.56] would occur. From [26, Theorem 11.116],  $|G| < 16g^2$ , a contradiction. Therefore, if  $P_\infty \in o_\infty$  and  $P_0 \in o_0$  then there exists  $w \in G$  taking  $P_\infty$  to  $P_0$ . Take two nontrivial elements  $r_\infty, r_0 \in Q$  fixing  $P_\infty$  and  $P_0$ , respectively. The conjugate  $r$  of  $r_\infty$  by  $w$  fixes  $P_0$ . Hence both  $r$  and  $r_0$  are in the stabilizer of  $P_0$  in  $G$ . From [26, Lemma 11.6], a  $p$ -subgroup  $R$  of  $G$  contains both  $r$  and  $r_0$ . Since the conjugate  $Q'$  of  $Q$  by  $w$  is a Sylow  $p$ -subgroup of  $G$ ,  $R$  has non-trivial elements from both two Sylow  $p$ -subgroups  $Q$  and  $Q'$ . Since  $G$  is a group in which any two distinct Sylow  $p$ -subgroup have trivial intersection, it turns out that  $Q = Q'$ , that is,  $w \in N_G(Q)$ . This is a contradiction as  $o_\infty$  is a  $N_G(Q)$ -orbit.  $\square$

**Lemma 4.8.** *Let  $G$  be a subgroup of  $\text{Aut}(\mathcal{X})$  with a nontrivial  $p$ -subgroup  $Q$  that satisfies the following properties.*

- (i)  $Z(G)$  has a nontrivial element  $g$  of order  $t$  with  $t < p$ ,
- (ii) *The normalizer of  $Q$  in  $G$  contains a subgroup  $N$  of order larger than  $|Q|t$  such that  $N = Q \rtimes M$  with an abelian group  $M$  of order prime to  $p$  containing  $g$ .*

*If  $\bar{\mathcal{X}} = \mathcal{X}/\langle g \rangle$  has zero  $p$ -rank and  $\tilde{\mathcal{X}} = \mathcal{X}/Q$  is rational then  $\mathcal{X}$  has also zero  $p$ -rank.*

*Proof.* Let  $U = \langle g \rangle$ . The quotient group  $\bar{Q} = QU/U$  is a  $p$ -subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ . Since  $\gamma(\bar{\mathcal{X}}) = 0$ , there exists a point  $\bar{P} \in \bar{\mathcal{X}}$  fixed by  $\bar{Q}$  but no nontrivial element in  $\bar{Q}$  fixes a point of  $\bar{\mathcal{X}}$  other than  $\bar{P}$ . Let  $o$  be the  $U$ -orbit in  $\mathcal{X}$  lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $|o| \leq t$  and  $t < p$  by (ii),  $Q$  fixes  $o$  pointwise. No point  $R \in \mathcal{X}$  other than those in  $o$  is fixed by  $Q$ , otherwise the point  $\bar{R}$  lying under  $R$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$  would be a fixed point of  $\bar{Q}$  distinct from  $\bar{P}$ . Therefore,  $N$  preserves  $o$ . From (ii),  $|o| \leq t < |M|$ . Hence, some nontrivial element  $m \in M$  fixes a point in  $o$ . Since  $M$  is abelian,  $m$  fixes  $o$  pointwise.

Furthermore, the cover  $\mathcal{X}|\tilde{\mathcal{X}}$  totally ramifies at the points of  $\tilde{\mathcal{X}}$  lying under those in  $o$  while it is unramified elsewhere. Now look at the action of the quotient group  $\tilde{N} = N/Q$  as a subgroup of  $\text{Aut}(\tilde{\mathcal{X}})$ . In the natural group homomorphism  $N \mapsto \tilde{N}$ , the image  $\tilde{m}$  of  $m$  is a nontrivial automorphism of  $\tilde{\mathcal{X}}$  which fixes each of the  $|o|$  points of  $\tilde{\mathcal{X}}$  lying under the points of  $o$  in the cover  $\mathcal{X}|\tilde{\mathcal{X}}$ . Since  $\tilde{\mathcal{X}}$  is rational,  $\tilde{N}$  is isomorphic to a subgroup of  $PGL(2, \mathbb{K})$ . Moreover,  $\tilde{N}$  is abelian by  $M \cong \tilde{N}$ . From Lemma 2.1,  $\tilde{N}$  is a cyclic group of order prime to  $p$  and hence it fixes exactly two points in  $\tilde{\mathcal{X}}$ , and no nontrivial element of  $\tilde{N}$  fixes a further point in  $\tilde{\mathcal{X}}$ . In particular, the image  $\tilde{g}$  of  $g$  has exactly two fixed points in  $\tilde{\mathcal{X}}$ , and they are also the fixed points of  $\tilde{m}$ . From this,  $|o| \leq 2$ . If equality holds then both points in  $o$  must be fixed by  $N$ . But this is impossible since  $o$  is an  $U$ -orbit and  $U \leq N$ . Therefore,  $|o| = 1$ , and hence  $Q$  has exactly one fixed point in  $\mathcal{X}$ . Since  $\gamma(\tilde{\mathcal{X}}) = 0$ , Lemma yields that  $\gamma(\mathcal{X}) = 0$  also holds.  $\square$

## 5. SOME LOW DIMENSIONAL LINEAR GROUPS AS AUTOMORPHISM GROUPS OF CURVES

For a prime-power  $q = d^k$  with an odd prime  $d$ , let  $W$  denote one of the following non-solvable linear groups

$$(9) \quad PSL(2, q), PGL(2, q), \text{ with } q \geq 5, PSU(3, q), PGU(3, q), PSL(3, q), PGL(3, q).$$

Choose a Sylow  $d$ -subgroup  $Q$  of  $W$ . If  $W \neq PSL(3, q), PGL(3, q)$  then the normalizer  $H$  of  $Q$  is a semidirect product  $Q \rtimes C_m$  with a cyclic complement  $C_m$  of order  $m$ . Here  $(|Q|, m)$  is  $(q, \frac{1}{2}(q-1))$ , or  $(q, q-1)$ , or  $(q^3, (q^2-1)/\mu)$ , or  $(q^3, q^2-1)$  according as  $W$  is  $PSL(2, q)$ , or  $PGL(2, q)$ , or  $PSU(3, q)$  or  $PGU(3, q)$  where  $\mu = \gcd(3, q+1)$ . In these cases,  $W$  has property (ii) of Lemma 4.7. Some but not all of these facts remain true for  $PSL(3, q)$  (and  $PGL(3, q)$ ). For  $PSL(3, q)$  with  $q = d^k$  and  $d > 2$  prime, the normalizer  $H$  of a Sylow  $d$ -subgroup  $Q$  is a semidirect product of  $Q$  by  $C_{q-1} \times C_{(q-1)/\mu}$  where  $\mu$  stands for 3 or 1 according as 3 divides  $q-1$  or does not. The same holds for  $PGL(3, q)$  with  $\mu = 1$  for any  $q$ .  $PSL(3, q)$  (and hence  $PGL(3, q)$ ) does not enjoy property (ii) of Lemma 4.7.

**Lemma 5.1.** *For  $W \neq PSL(3, q), PGL(3, q)$ , let  $W$  be isomorphic to a subgroup of  $\text{Aut}(\mathcal{X})$ . If*

$$(10) \quad |W| > 900g^2$$

*then  $\mathcal{X}$  has zero  $p$ -rank and  $q$  is a power of  $p$ .*

*Proof.* For a Sylow  $d$ -subgroup  $Q$  of  $W$ , let  $H$  be the normalizer of  $Q$  in  $W$ . Assumption  $|G| > 900g^2$  yields  $|H| > 30(g-1)$ . As  $900 > 16$ , the assertions follow from Lemmas 4.7 and 4.1.  $\square$

As it is known,  $\text{Aut}(W) = P\Gamma L(2, q)$  when  $W = PSL(2, q)$ , or  $W = PGL(2, q)$  while  $\text{Aut}(W) = P\Gamma L(3, q)$  when  $W = PSU(3, q)$  or  $W = PGU(3, q)$ ; see for instance [47, Sections 3.3.4, 3.6.3]. So,  $W \leq \text{Aut}(W)$  may be assumed. Let  $G$  any subgroup of  $\text{Aut}(W)$  containing  $W$ .

**Remark 5.2.** In the natural representation of  $P\Gamma L(2, q)$  as a semilinear group on the projective line  $PG(1, q)$  over  $\mathbb{F}_q$ , the subgroup  $PSL(2, q)$  acts on  $PG(1, q)$  as doubly transitive permutation group such that its stabilizer  $M$  of the origin  $O$  and the infinite point  $\infty$  has order  $\frac{1}{2}(q-1)$  and consists of all permutations  $x \mapsto ax$  with a non-zero quadratic element  $a$  in  $\mathbb{F}_q$ . The stabilizer of  $\infty$  is  $H = Q \rtimes M$  where  $Q$  is the Sylow  $d$ -subgroup of  $PSL(2, q)$  consisting of all translations  $x \mapsto x + c$  with  $c \in \mathbb{F}_q$ . If a subgroup  $G$  of  $P\Gamma L(2, q)$  contains  $PSL(2, q)$  then the stabilizer of  $\infty$  in  $G$  is  $G_{\infty, O} \rtimes Q$  where  $G_{\infty, O}$  is the stabilizer of  $\infty$  and  $O$  in  $G$ , and  $M$  is a normal subgroup of  $G_{\infty, O}$ . Suppose that  $G$  contains  $PSL(2, q)$  properly. Then  $G_{\infty, O}$  has an element  $v$  other than those in  $M$ . If  $v \in PGL(2, q)$  then  $G$  also contains  $PGL(2, q) = \langle PSL(2, q), v \rangle$ . Since  $PGL(2, q)$  is the only linear subgroup of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$  properly, it turns out that if  $G$  is not linear then  $G_{\infty, O}$  contains a permutation  $\varphi : x \mapsto \alpha x^\sigma$  where  $\alpha \in \mathbb{F}_q$  and  $\sigma$  is a non-trivial automorphism of  $\mathbb{F}_q$ . Then  $\varphi\psi_a \neq \psi_a\varphi$  for  $\psi_a : x \mapsto ax$  with  $a \in \mathbb{F}_q$  such that  $\sigma(a) \neq a$ . Hence  $G_{\infty, O}$  is not abelian. We show that  $G_{\infty, O}$  is neither dihedral for  $|G| > 720$ . Since  $M$  is a cyclic subgroup of order  $\frac{1}{2}(q-1)/2 \geq 4$ , the index 2 cyclic subgroup of any dihedral group containing  $M$  also contains  $M$ . As we have already showed the centralizer of  $M$  does not contain  $\varphi$ . Therefore, if  $G_{\infty, O}$  is assumed to be dihedral then  $\varphi$  is an element in the coset of the index 2 cyclic subgroup of  $G_{\infty, O}$ . Thus  $\varphi^2 = 1$ , that is,  $\sigma$  is involutory and  $\alpha^{\sigma+1} = 1$ . Furthermore,  $\varphi\psi_a\varphi = (\psi_a)^{-1} = \psi_{a^{-1}}$  holds for every  $a \in D$ . Therefore,  $a^{\sigma+1} = 1$  for every  $a \in D$ . Since  $|D| = \frac{1}{2}(q-1)$  this occurs if and only if  $d = 3, q = 9$ . Hence, either  $G = P\Gamma L(2, 9)$ , and  $|G| = 1440$ , or  $G$  has order 720. The former case  $G = P\Gamma L(2, 9)$ , as  $P\Gamma L(2, 9)_{\infty, O}$  is a semi-dihedral group of order 16. In the latter case,  $G$  is one of the two subgroups of  $P\Gamma L(2, 9)$  of order 720, other than  $PGL(2, 9)$ . Therefore, if  $G_{\infty, O}$  is dihedral then  $|G| = 720$ .

The same results hold for  $PTU(3, q)$ . Let  $D$  be the subgroup of index  $\mu$  in the multiplicative group of  $\mathbb{F}_{q^2}$ . In the natural representation of  $PTU(3, q)$  as a semilinear group on the set of all  $\mathbb{F}_{q^2}$ -rational points of the Hermitian curve  $\mathcal{H}$  its canonical equation  $y^q + y = x^{q+1}$ , a Sylow  $d$ -subgroup  $Q$  of  $PSU(3, q)$  consists of all maps  $(x, y) \mapsto (x + a, y + a^q x + b)$  with  $a, b \in \mathbb{F}_{q^2}$  and  $b^q + b = a^{q+1}$ . The subgroup  $PSU(3, q)$  acts on  $\mathcal{H}$  as doubly transitive permutation group such that its stabilizer  $M$  of the origin  $O = (0, 0)$  and the infinite point  $\infty$  of the  $y$ -axis has order  $(q^2-1)/\mu$  and it consists of all maps  $\psi_{a, b} : (x, y) \mapsto (ax, by)$  with  $a \in D$  and  $b = \frac{1}{2}a^{q+1}$ . Suppose that a subgroup  $G$  of  $PTU(3, q)$  contains  $PSU(3, q)$  properly. Then the stabilizer  $G_{\infty, O}$  of  $G$  has an element  $v$  other than those in  $M$ . If  $v \in PGU(3, q)$  (and  $\mu = 3$ ) then  $G$  also contains  $PGU(3, q) = \langle PSU(3, q), v \rangle$ . Since  $PGU(3, q)$  is the only linear subgroup of  $PTU(3, q)$  containing  $PSU(3, q)$

properly, it turns out that if  $G$  is not linear then  $G_{\infty,O}$  contains a map  $\varphi : (x, y) \mapsto (\alpha x^\sigma, \beta y^\sigma)$  where  $\alpha \in D$ ,  $\beta = \frac{1}{2}\alpha^{q+1}$  and  $\sigma$  is a non-trivial automorphism of  $\mathbb{F}_q$ . Then  $\varphi\psi_{a,b} \neq \psi_{a,b}\varphi$  for  $a \in \mathbb{F}_q$  such that  $\sigma(a) \neq a$ . Hence  $G_{\infty,O}$  is not abelian. We show that  $G_{\infty,O}$  is neither dihedral. Since  $M$  is a cyclic subgroup of order  $(q^2 - 1)/\mu \geq 3$ , the index 2 cyclic subgroup of any dihedral group containing  $M$  also contains  $M$ . The centralizer of  $M$  does not contain  $\varphi$ . Therefore, if  $G_{\infty,O}$  is dihedral by absurd, then  $\varphi$  is in the coset of the index 2 cyclic subgroup of  $G_{\infty,O}$ . Hence  $\sigma$  is involutory,  $\alpha^{\sigma+1} = 1$ , and  $\varphi\psi_{a,b}\varphi = (\psi_{a,b})^{-1} = \psi_{a^{-1},b^{-1}}$  holds for every  $\psi_{a,b} \in M$ . From this,  $a^{\sigma+1} = 1$  follows for every  $a \in D$ . Since  $|D| = (q^2 - 1)/\mu$  this yields  $d^h + 1 = (d^{2k} - 1)/\mu$  with  $\sigma = d^h$ . As  $\mu = 1$  or  $\mu = 3$ , this is impossible. Therefore  $G_{\infty,O}$  is not dihedral.

**Lemma 5.3.** *Let  $G$  be a subgroup of  $\text{Aut}(W)$  containing  $W$  where  $W$  is one of the groups on the list (9). If  $G$  is also a subgroup of  $\text{Aut}(\mathcal{X})$  up to an isomorphism, and*

$$(11) \quad |G| > 900c\mathfrak{g}^2$$

with

$$c = \begin{cases} \frac{2k(q+1)}{(q-1)q} & \text{if } W = PSL(2, q), \\ \frac{k(q+1)}{(q-1)q} & \text{if } W = PGL(2, q), \\ \frac{2k\mu(q^3+1)}{(q^2-1)q^3} & \text{if } W = PSU(3, q), \\ \frac{2k(q^3+1)}{(q^2-1)q^3} & \text{if } W = PGU(3, q), \\ \frac{k\mu(q^2+q+1)(q+1)}{(q^2-1)q^3} & \text{if } W = PSL(3, q), \\ \frac{k(q^2+q+1)(q+1)}{(q^2-1)q^3} & \text{if } W = PGL(3, q), \end{cases}$$

then  $G$  is linear, and  $W \neq PSL(3, q), PGL(3, q)$ .

*Proof.* We begin with case  $W = PSL(2, q)$ . Let  $Q$  be a Sylow  $d$ -subgroup of  $PSL(2, q)$  and  $H$  its normalizer in  $PSL(2, q)$ . We may assume that  $Q$  and  $H$  are taken as in Remark 5.2. Then  $T = G_\infty$  is a subgroup of  $G$  containing  $H$  as a normal subgroup such that  $T = Q \rtimes G_{\infty,O}$ . Assume that  $G$  is nonlinear. From Remark 5.2,  $G_{\infty,O}$  is not cyclic and it is dihedral only for  $d = 3$  and  $|G| = 720$ . On the other hand,  $k \geq 2$  and  $|G| = \frac{1}{2}h(q-1)q(q+1)$  where  $h > 1$  is a divisor of  $k$ . Assumption  $|G| > 900c\mathfrak{g}^2$  yields

$$(12) \quad |H| = \frac{1}{2}(q-1)q > 30\sqrt{\frac{c(q-1)q}{2h(q+1)}}\mathfrak{g} > 30\mathfrak{g}.$$

By (11),  $H$  satisfies the hypotheses of Lemma 4.1. By Lemma 4.5,  $G_{\infty,O}$  is either cyclic or dihedral. Since  $|G| > 720$  this is impossible.

Now, let  $W = PSU(3, q)$ . By the above argument applied to a subgroup  $G$  of  $PTL(3, q)$  containing  $PSU(3, q)$  properly, Remark 5.2 shows that  $T = G_\infty$  is a subgroup of  $G$  containing  $H$  as a normal subgroup such that  $T = Q \rtimes G_{\infty,O}$  where  $G_{\infty,O}$  is neither cyclic nor dihedral when  $G$  is nonlinear. On the other hand,  $|G| = \frac{1}{\mu}h(q^2-1)q^3(q^3+1)$  where  $h$  is a divisor of  $2k$ . Assumption  $|G| > 900c\mathfrak{g}^2$  yields

$$(13) \quad |H| = \frac{1}{\mu}(q^2-1)q^3 > 30\sqrt{\frac{c(q^2-1)q^3}{\mu h(q^3+1)}}\mathfrak{g} > 30\mathfrak{g}.$$

By (11),  $H$  satisfies the hypotheses of Lemma 4.1. From Lemma 4.5,  $T = Q \rtimes G_{\infty,O}$  where  $V$  is either cyclic or dihedral, a contradiction.

Finally, let  $W = PSL(3, q)$ . Then  $|W| = \frac{1}{\mu}h(q-1)^2q^3(q^2+q+1)(q+1)$  where  $h$  is a divisor of  $k$ . Then

$$(14) \quad |H| = \frac{1}{\mu}(q-1)^2q^3 > 30\sqrt{\frac{c(q-1)^2q^3}{\mu h(q^2+q+1)(q+1)}}\mathfrak{g} > 30\mathfrak{g}.$$

By (10), the hypotheses on  $H$  in Lemma 4.1 are satisfied. From Lemma 4.5,  $T = Q \rtimes V$  where  $V$  is either cyclic or dihedral. However,  $H$  contains the direct product of two cyclic groups, and hence  $V$  is neither cyclic, nor a dihedral group. This contradiction shows that  $W \neq PSL(3, q)$ . A similar argument shows that  $W = PGL(3, q)$  cannot occur.  $\square$

**Remark 5.4.** In Lemma 5.3  $c \leq 1$  holds in each case.

**Remark 5.5.** In some but not all cases, Lemma 5.3 follows from the Abhyankar Conjecture under a bit weaker condition, namely when  $|G| > 24g^2$ . In fact, this condition yields that either  $G$  has a unique non-tame short orbit, or it has exactly two short orbits one tame, the other non-tame; see [26, Theorems 11.56, 11.116]. Furthermore, the quotient curve  $\mathcal{X}/G$  is rational, and the Abhyankar Conjecture applies to  $G$ . Observe that  $G \geq W$  with a non-abelian simple group  $W$ . In the former case,  $G$  is generated by its Sylow  $p$ -subgroups and hence  $G \geq W$  implies  $G = W$ , and  $G$  is linear. In the latter case,  $G/W$  is a cyclic group. For instance, this occurs when  $G$  does not contain  $PGL(2, q)$  or  $PSU(3, q)$ . On the other hand,  $G/W$  contains two involutions and hence is not cyclic when  $q$  is a quadrate and  $G$  contains  $PGL(2, q)$ , or  $PSU(3, q)$ .

The following lemma shows that the hypothesis  $W \neq PSL(3, q), PGL(3, q)$  in Lemma 5.1 is meaningful.

**Lemma 5.6.** *If  $W = PSL(3, q)$  with  $q > 3$  is a subgroup of  $\text{Aut}(\mathcal{X})$  then  $|G| < 72g^2$ .*

*Proof.* As we have already observed  $H = Q \rtimes (C_{q-1} \times C_{(q-1)/\mu})$ . Let  $M$  be the subgroup of  $C_{(q-1)/\mu}$  of index 2. Then the factor group  $\bar{T} = (C_{q-1} \times C_{(q-1)/\mu})/M$  has order  $2(q-1)$ . Here  $\bar{T}$  is a non-cyclic abelian group of order greater than 4. Obviously, the subgroup  $U = Q \rtimes M$  is a normal subgroup of  $H$ . Therefore,  $\bar{H} = H/U$  is an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/U$ . Since  $\bar{H} \cong \bar{T}$ , no subgroup of  $PGL(2, \mathbb{K})$  is isomorphic to  $\bar{H}$  by Lemma 2.1. Therefore  $\bar{\mathcal{X}}$  is not rational. If  $\bar{\mathcal{X}}$  is elliptic then  $U$  has a short orbit  $o$ , and for a point  $P \in o$ , the contribution of  $o$  to the different  $D(\mathcal{X}|\bar{\mathcal{X}})$  is at least  $|o|(|U_P| - 1) \geq \frac{1}{2}|o|U_P| = \frac{1}{2}|U|$ ; see [26, Theorem 11.70]. Assume that  $o$  is the unique short orbit of  $U$ . Then  $o$  is also an  $H$ -orbit. Thus  $|H_P|/|U_P| = |H|/|U|$  whence

$$|H_P U/U| = \frac{|H_P U|}{|U|} = \frac{|H_P||U|}{|H_P \cap U|} \cdot \frac{1}{|U|} = \frac{|H_P|}{|U_P|} = \frac{|H|}{|U|} = |\bar{T}| = 2(q-1).$$

This shows that  $H_P U/U$  has order  $2(q-1)$ . Furthermore,  $H_P U/U$  viewed as an automorphism group of  $\bar{\mathcal{X}}$  fixes the point  $\bar{P} \in \bar{\mathcal{X}}$  lying under  $o$ . But then  $q < 5$ , as  $\bar{\mathcal{X}}$  is elliptic; see [26, Theorem 11.94]. Therefore, there is another such orbit, and the Hurwitz genus formula gives  $2(g-1) \geq |U|$  whence

$$g-1 \geq \frac{1}{2}|U| = \frac{1}{4} \frac{q-1}{\mu} q^3.$$

This holds true for  $g(\bar{\mathcal{X}}) \geq 2$ , by the Hurwitz genus formula. Therefore,

$$72g^2 > 72(g-1)^2 \geq \frac{24}{16\mu} \frac{(q-1)^2}{\mu} q^6 \geq \frac{3}{2} q^3 q^3 \frac{(q-1)^2}{\mu} > (q^2 + q + 1)(q+1)q^3 \frac{(q-1)^2}{\mu} = |G|,$$

a contradiction with the hypothesis of the lemma.  $\square$

A variant of the proof of Lemma 5.3 can be used to prove a similar result for the group  $SL(2, q)$  with  $q = d^k$  and  $d$  prime. In the natural representation of  $SL(2, q)$  as a linear group of the vector space  $V(2, \mathbb{F}_q)$ , a Sylow  $d$ -subgroup is the subgroup  $Q$  consisting of all maps  $(x, y) \mapsto (x + ry, y)$  with  $r \in \mathbb{F}_q$ , and the normalizer of  $Q$  in  $SL(2, q)$  is the semidirect product  $Q \rtimes M$  where  $M \cong C_{q-1}$  consists of all transformations  $(x, y) \mapsto (ax, a^{-1}y)$  with  $a \in \mathbb{F}_q^*$ .

**Lemma 5.7.** *Let  $G$  be a group with commutator subgroup  $G' = SL(2, q)$  such that the centralizer of  $G'$  in  $G$  has order 2. If  $G$  is also a subgroup of  $\text{Aut}(\mathcal{X})$ , and*

$$(15) \quad |G| > 900g^2$$

*then  $\mathcal{X}$  has zero  $p$ -rank and  $q$  is a power of  $p$ .*



*Proof.* For every  $g \in G$ , let  $\varphi_g$  denote the automorphism of  $G'$  taking the element  $h \in G'$  to its conjugate  $h^g$ . The map from  $G$  to  $\text{Aut}(G')$  which takes  $g$  to  $\varphi_g$  is a group homomorphism whose kernel consists of the elements in  $G$  which centralize  $G'$ . Hence,  $|G| = 2|L|$  with a subgroup  $L$  of  $\text{Aut}(G')$ . From  $\text{Aut}(SL(2, q)) \cong P\Gamma L(2, q)$ , we have that  $|G| \leq 2k(q+1)q(q-1)$  where  $q = d^k$  and  $d$  is an odd prime  $d$ . Observe that if  $4k(q+1) > (q-1)q$  then  $q = 3, 5, 9$ , but for these values of  $q$ ,  $|G| \leq 2880 < 3600 \leq 900\mathfrak{g}^2$ . Hence

$$(16) \quad \frac{4k(q+1)}{(q-1)q} \leq 1.$$

For the normalizer  $H = Q \rtimes U$  of  $Q$  in  $SL(2, q)$ , assumption  $|G| > 900\mathfrak{g}^2$  yields

$$(17) \quad |H| = (q-1)q > 30\mathfrak{g},$$

which shows that  $H$  satisfies the hypotheses in Lemma 4.1. Therefore,  $d = p$  and the quotient curve  $\tilde{\mathcal{X}} = \mathcal{X}/Q$  is rational. Take a point  $P$  from one of the short orbits  $\Omega_1$  of  $H$ . Then  $|H_P| = |H||Q_P| = (q-1)p^r$  with a positive integer  $r$ . By absurd,  $\mathcal{X}$  has positive  $p$ -rank and hence (i) of Lemma 4.1 occurs. We prove that Lemma 4.8 applies to  $G$  where  $g$  is the central involution of  $G'$ . Obviously,  $g \in Z(G)$  as  $G'$  is a characteristic subgroup of  $G$ .

It remains to show that the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/V$  with  $V = \langle g \rangle$  has zero  $p$ -rank. For this purpose, we need three facts:

- (i)  $\bar{G} = G/V$  isomorphic to a subgroup of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$ .
- (ii)  $\bar{G}$  is a subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ .
- (iii) Let  $\bar{H} = H/V$ . If  $\bar{P}$  is a point of  $\bar{\mathcal{X}}$  lying under  $P \in \Omega_1$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ , then  $|\bar{H}_{\bar{P}}| = \frac{1}{2}(q-1)p^r$  with a positive integer  $r$ .

By (16), Lemma 5.3 for  $W = PSL(2, q)$  applies to  $\bar{G}$ . Therefore, either  $\bar{G} = PSL(2, q)$ , or  $\bar{G} = PGL(2, q)$ . If  $\bar{\mathfrak{g}} = \mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  then  $\mathfrak{g} - 1 \geq 2(\bar{\mathfrak{g}} - 1)$  and hence

$$|\bar{G}| = \frac{1}{2}|G| \geq 900\mathfrak{g}^2 \geq 900 \cdot \frac{1}{2}(2\bar{\mathfrak{g}} - 1)^2 > 900\bar{\mathfrak{g}}^2,$$

which yields  $\bar{\mathfrak{g}} = 0$  by Lemma 5.1 applied to  $\bar{G}$ . If  $\bar{\mathcal{X}}$  is elliptic, (iii) together with [26, Remark 11.95] yield  $p = 3$  and  $\frac{1}{4}(q-1) = |\bar{H}_P| \in \{6, 12\}$  whence  $q = 9$ . On the other hand  $|PGL(2, 9)| = 2|PSL(2, 9)| = 720$ . Hence  $|G| \leq 1440 < 900\mathfrak{g}^2$  as  $\mathfrak{g} \geq 2$ . Therefore,  $\mathcal{X}$  is not elliptic.  $\square$

## 6. STRUCTURE OF AUTOMORPHISM GROUPS OF CURVES OF EVEN GENUS

In this section,  $\mathbb{K}$  is an algebraically closed field of odd characteristic  $p$ ,  $\mathcal{X}$  is an algebraic curve whose genus  $\mathfrak{g}$  is a (nonzero) even integer, and  $G$  is an automorphism group of  $\mathcal{X}$ .

A key property is given in the following lemma.

**Lemma 6.1.** *If  $G$  has even order, then any 2-subgroup of  $G$  has a cyclic subgroup of index 2.*

*Proof.* Let  $U$  be a subgroup of  $\text{Aut}(\mathcal{X})$  of order  $d = 2^u \geq 2$ . From the Hurwitz genus formula applied to  $U$ ,

$$2\mathfrak{g} - 2 = 2(p-2)p^{n-1} = 2^u(2\bar{\mathfrak{g}} - 2) + \sum_{i=1}^m (2^u - \ell_i)$$

where  $\bar{\mathfrak{g}}$  is the genus of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/U$  and  $\ell_1, \dots, \ell_m$  are the short orbits of  $U$  on  $\mathcal{X}$ . Since  $2(p-2)p^{n-1} \equiv 2 \pmod{4}$  while  $2^u(2\bar{\mathfrak{g}} - 2) \equiv 0 \pmod{4}$ , some  $\ell_i$  ( $1 \leq i \leq m$ ) must be either 1 or 2. Therefore,  $U$  or a subgroup of  $U$  of index 2 fixes a point of  $\mathcal{X}$  and hence is cyclic.  $\square$

**Remark 6.2.** From Lemma 6.1 and [28, Chapter I, Satz 14.9], any nontrivial 2-subgroup  $U$  of  $G$  is either cyclic, or the direct product of a cyclic group by a group of order 2, or a generalized quaternion group, or dihedral, or semidihedral, or a modular maximal-cyclic group (also called type (3) with Huppert's notation). Furthermore,  $U$  is either abelian, or a generalized quaternion group, or it has at least one involution other than the unique involution in the center  $Z(U)$  of  $U$ . Also, if  $U$  is dihedral, semidihedral or a generalized



quaternion group then its center has order 2. If  $U$  is a modular maximal-cyclic group then it has exactly four elements of order 4 and hence it does not contain a generalized quaternion group.

The following lemma shows that a Sylow 2-subgroup of  $G$  has 2-rank at most 2.

**Lemma 6.3.**  *$G$  contains no elementary abelian 2-subgroup of order 8.*

*Proof.* The assertion is a corollary of the classification theorem quoted in Remark 6.2.  $\square$

**Lemma 6.4.** *If  $G$  has a minimal normal subgroup  $N$  of order 2 then  $G = O(G) \rtimes S_2$ , unless a Sylow 2-subgroup of  $G$  is a generalized quaternion group.*

*Proof.* Let  $S_2$  be a Sylow 2-subgroup of  $G$ . Then  $S_2$  contains  $N$ , as  $N$  lies in the center of  $G$ . Assume that  $S_2$  is neither cyclic, nor a generalized quaternion group. By Remark 6.2,  $S_2$  has a cyclic subgroup  $U$  of index 2 such that  $S_2 \setminus U$  contains an involution  $v$ . From the Thompson transfer lemma, [44, Lemma 5.38], see also [17, Proposition I.21], either  $G$  has a subgroup of index 2 containing  $U$ , or  $v$  is conjugate to an involution in  $U$ . The latter case cannot actually occur in our situation, since the normal subgroup  $N$  consists of the unique involution of  $U$  together with the identity. Therefore,  $G$  has a subgroup  $M$  of By [28, Chapter I, Aufgaben I.21],  $M = O(M) \rtimes U$ . Since  $M$  is a normal subgroup of  $G$  and  $O(M)$  is a characteristic subgroup of  $M$ ,  $O(M)$  is a normal subgroup of  $G$ . Moreover,  $[G : O(M)] = 2[M : O(M)]$  yields  $O(G) = O(M)$ . From  $M = O(G) \rtimes U$ , we have that  $|O(G)|$  and  $[G : O(G)]$  are co-primes. By [28, Chapter I, Satz 17.5],  $G = O(G) \rtimes S_2$ . This remains true when  $S_2$  is cyclic; see [28, Chapter I, Aufgaben I.21].  $\square$

**Remark 6.5.**  $SL^\pm(2, q)$  denotes the subgroup of  $GL(2, q)$  consisting of all matrices with determinant equal to  $\pm 1$ . The center of  $SL^\pm(2, q)$  has order 2 and it is a minimal normal subgroup of  $SL^\pm(2, q)$ . Furthermore, a Sylow 2-subgroup of  $SL^\pm(2, q)$  contains at least two involutions, and hence it cannot be a generalized quaternion group, more precisely, it is a semidihedral group. This together with Lemma 6.4 imply that  $\text{Aut}(\mathcal{X})$  has no subgroup isomorphic to  $SL^\pm(2, q)$ . Another linear group containing  $SL(2, q)$  as an index 2 subgroup is  $SU^\pm(2, q)$  which consist of all matrices of  $GU(2, q)$  with determinant  $\pm 1$ . Its Sylow 2-subgroups are generalized quaternion groups. Indeed,  $SU^\pm(2, q)$  can be isomorphic to a subgroup of  $\text{Aut}(\mathcal{X})$  of some curve  $\mathcal{X}$  of even genus; see Section 9.

**Lemma 6.6.** *If  $G$  has a minimal normal subgroup  $N$  of order 4, then either  $G$ , or a normal subgroup of  $G$  of index 3, has the following property:  $G = O(G) \rtimes S_2$  where  $S_2$  is the direct product of a cyclic group by a group of order 2.*

*Proof.* The centralizer  $C_G(N)$  of  $N$  in  $G$  is a normal subgroup such that  $G/C_G(N)$  is isomorphic to a subgroup of  $\text{Sym}_3$ . Therefore, either  $G$ , or a normal subgroup of  $G$  of index 3, has the property that each of its subgroups of odd order is contained in  $C_G(N)$ . If the latter case occurs, replace  $G$  with that normal subgroup of index 3.

Let  $S_2$  be a Sylow 2-subgroup of  $G$ . Then  $N$  lies in  $S_2$ . Furthermore, since  $N = C_2 \times C_2$ , Remark 6.2 shows that  $S_2$  must be a direct product  $C_{2^m} \times C_2$ . Hence, the factor group  $S_2/N$  is a cyclic group. Therefore, the factor group  $\bar{G} = G/N$  has a cyclic Sylow 2-subgroup  $\bar{U}$ . By [28, Chapter I, Aufgaben I.21],  $\bar{G} = O(\bar{G}) \rtimes \bar{U}$ . Let  $L$  be the normal subgroup of  $G$  such that  $\varphi(L) = O(\bar{G})$  where  $\varphi$  is the natural homomorphism  $G \mapsto \bar{G}$ . Then  $|L| = 4|O(\bar{G})|$ . Moreover, since  $N$  is a normal subgroup of  $L$  of order 4, [28, Chapter I, Satz 17.5] shows that  $L$  contains a subgroup  $T \cong O(\bar{G})$  such that  $L = N \rtimes T$ . More precisely,  $L = N \times T$  as  $N$  centralizes  $T$ . Therefore,  $T = O(L)$ , and hence  $O(L)$  is a characteristic subgroup of  $L$ . Therefore,  $T$  is a normal subgroup of  $G$  of odd order such that  $|T|$  and  $[G : T]$  are co-primes. In particular,  $T = O(G)$ . By [28, Chapter I, Satz 17.5],  $G = O(G) \rtimes S_2$ .  $\square$

**Lemma 6.7.** *If  $G$  has a non-abelian minimal normal subgroup  $N$  then  $N$  is a simple group and one the following cases occurs.*

- (i)  $N \cong \text{PSL}(2, q)$  with  $q \geq 5$  odd, and a Sylow 2-subgroup of  $N$  is dihedral;

- (ii)  $N \cong PSL(3, q)$  with  $q \equiv 3 \pmod{4}$ , and a Sylow 2-subgroup of  $N$  is semidihedral;
- (iii)  $N \cong PSU(3, q)$  with  $q \equiv 1 \pmod{4}$ , and a Sylow 2-subgroup of  $N$  is semidihedral;
- (iv)  $N \cong \text{Alt}_7$ , and a Sylow 2-subgroup of  $N$  is dihedral;
- (v)  $N \cong M_{11}$ , the Mathieu group on 11 letters, and a Sylow 2-subgroup of  $N$  is semidihedral.

*Proof.*  $N$  is the direct product of pairwise isomorphic non-abelian simple groups  $M$ , see [28, Chapter I, Satz 9.13]. Since a Sylow 2-subgroup of  $M$  is neither cyclic nor a generalized quaternion group by the Brauer-Suzuki theorem, see [8], a Sylow 2-subgroup of  $M$  has 2-rank at least 2. If that the direct product had more than one factors, then a Sylow 2-subgroup of  $N$  would have 2-rank larger than 2, contradicting Lemma 6.3. Hence  $N = M$ . By a result due to Alperin [3], a Sylow 2-subgroup of a non-abelian simple group with 2-rank equal to 2 is either dihedral, or semidihedral, or wreathed, or isomorphic to a Sylow 2-subgroup of  $U_3(4)$ . By Lemma 6.1, the latter two cases cannot occur in our situation. Now, further deep results from Group theory apply, see [4, 19, 20, 46], determining the structure of  $N$ . The possibilities are listed in (i), ..., (iv).  $\square$

If a group  $G$  contains a nontrivial normal subgroup of odd order, the *odd core* of  $G$  is its maximal normal subgroup of odd order. Otherwise,  $G$  is a *odd core-free* group. For odd core-free groups  $G$  the Lemmas 6.4 are 6.7 can be refined.

**Lemma 6.8.** *If  $G$  is an odd core-free group with generalized quaternion Sylow 2-subgroups, then its commutator subgroup  $G'$  is isomorphic to  $SL(2, q)$  where  $q = d^h$  with  $d \geq 5$  prime, apart from three cases:*

- (i)  $G$  is a generalized quaternion group,
- (ii)  $G$  is isomorphic to the unique perfect group of order 5040 and  $G/Z(G) \cong \text{Alt}_7$ ,
- (iii)  $G$  is isomorphic to the group named `SmallGroup(48, 28)` in the GAP-database.

*Proof.* If  $G$  is a 2-group, case (i) holds. From now on  $|G|$  is assumed to have some odd divisor.

From the Brauer-Suzuki theorem, [8],  $|Z(G)|$  has order 2. We point out that the factor group  $\bar{G} = G/Z(G)$  is also odd core-free. By absurd, let  $\bar{N}$  be a nontrivial normal subgroup of  $\bar{G}$  of odd order. Then there exists a normal subgroup  $N$  of  $G$  such that  $\varphi(N) = \bar{N}$  where  $\varphi$  is the natural homomorphism  $G \mapsto \bar{G}$ . Since  $G$  is odd core-free,  $N$  has even order. Since the involution  $z$  generating  $Z(G)$  is the unique involution in  $G$ ,  $N$  must contain  $z$ . Since  $|\bar{N}|$  is odd,  $|N|$  is twice of an odd number bigger than 1. Since  $z \in N$ , this yields  $N = Z(G) \times O(N)$ . Therefore,  $O(N)$  is nontrivial. Since  $N$  is a normal subgroup of  $G$ , this yields that also is  $O(N)$ , a contradiction. Hence  $\bar{G}$  is odd core-free. Furthermore, a Sylow 2-subgroup of  $\bar{G}$  is  $\bar{S}_2 = S_2/Z(S)$  which is a dihedral group as  $S_2$  a generalized quaternion group.

From the Gorenstein-Walter theorem, [19, 20],  $\bar{G}$  is either a dihedral group whose order is a power of 2 in which case (i) holds, or  $\bar{G} \cong \text{Alt}_7$ , or  $PSL(2, q) \leq \bar{G} \leq P\Gamma L(2, q)$  with  $q$  odd, up to a group-isomorphism. For  $q \geq 5$ ,  $PSL(2, q)$  is a perfect group, while the commutator subgroup of  $PSL(2, 3)$  is an elementary abelian group of order 4.

If  $q = 3$  then either  $\bar{G} \cong PSL(2, 3)$ , or  $\bar{G} \cong PGL(2, 3)$ . By direct GAP-aided computation,  $G \cong SL(2, 3)$  in the former case while if  $\bar{G} \cong PGL(2, 3)$ , the only possibility for  $G$  is the group `SmallGroup(48, 28)` in the GAP database. This gives (iii).

Suppose  $q \geq 5$ . As  $G'$  is a normal subgroup of  $G$ , and  $G$  is odd core-free,  $G'$  has even order. Since  $z$  is the unique involution of  $G$ ,  $z$  is contained in  $G'$ , that is,  $Z(G) \leq G'$ . Thus,  $G'/Z(G) = G'Z(G)/Z(G)$ . On the other hand,  $G'Z(G)/Z(G)$  is the commutator subgroup of  $\bar{G}$ , see [28, Hilfssatz 8.4, Chapter I], and, since  $q \geq 5$ , either  $G'/Z(G) \cong PSL(2, q)$ , or  $G'/Z(G) \cong \text{Alt}_7$ .

The commutator subgroup  $H$  of  $G'$  is a characteristic subgroup of  $G'$ , and hence a normal subgroup of  $G$ . Therefore,  $H$  has even order, and hence contains  $Z(G)$ . As before, this yields that either  $H/Z(G) \cong PSL(2, q)$ , or  $H/Z(G) \cong \text{Alt}_7$ . Since  $H \leq G'$ , this yields  $H = G'$  showing that  $G'$  is a perfect group, and hence  $G'$  is a stem extension of either  $PSL(2, q)$ , or  $\text{Alt}_7$ .

For  $q \neq 3, 9$ , the Schur multiplier of  $PSL(2, q)$  has order 2, and hence it has a unique stem extension which is  $SL(2, q)$ ; see [18, Chapter 10,  $IV_K$ ]. Therefore  $G' \cong SL(2, q)$  for  $q \neq 3, 9$ . Both  $PSL(2, 9)$  and

$\text{Alt}_7$  have a unique stem extension with center of order 2. In the former case, this extension is  $SL(2, q)$  and hence  $G' \cong SL(2, 9)$ . In the latter case it is the unique perfect group  $P$  of order 5040, and hence  $G' \cong P$ . From this, since  $|G| = 2|\bar{G}| = 5040 = |P| = |G'|$ , we also have  $G = G'$  whence (ii) follows.  $\square$

**Remark 6.9.** The proof of Lemma 6.8 can be shortened using [9, Proposition 4] stated without proof.

**Lemma 6.10.** *If  $G$  is an odd core-free group with commutator subgroup  $G' \cong SL(2, q)$  then the centralizer of  $G'$  in  $G$  has order 2.*

*Proof.* Since  $G'$  is a normal subgroup of  $G$ , the centralizer  $C_G(G')$  of  $G'$  in  $G$  is a normal subgroup of  $G$ . As  $G$  is odd core-free,  $C_G(G')$  has even order. By absurd,  $|C_G(G')| > 2$ . Therefore  $|C_G(G')|$  must be divisible by four, otherwise  $|C_G(G')|$  is twice an odd number and hence  $C_G(G') = Z(G') \times O(C_G(G'))$  where  $O(C_G(G'))$  is a characteristic subgroup of  $C_G(G')$  of odd order contradicting the hypothesis that  $G$  is odd core-free. Therefore,  $C_G(G')$  has a Sylow 2-subgroup  $R$  of order at least 4.

Take a Sylow 2-subgroup  $V$ , and let  $U = VR$ . Then  $|Z(U)| \geq 4$ , and  $|Z(V)| = 2$  yields  $U \not\cong V$ . From  $|Z(U)| \geq 4$ ,  $U$  is neither a generalized quaternion, nor a dihedral nor a semidihedral group. Also,  $U$  is not a modular maximal-cyclic group as the latter group has exactly four elements of order 4 while a generalized quaternion group has six elements of order 4. Therefore  $U \not\cong V$  cannot actually occur by Remark 6.2, and the assertion follows by absurd.  $\square$

**Lemma 6.11.** *If  $G$  is an odd core-free group with a non-abelian simple minimal normal subgroup, then one of the following cases occurs, up to group isomorphisms, where  $q$  is a prime power  $d^k$  with  $k$  odd:*

- (i)  $PSL(2, q) \leq G \leq P\Gamma L(2, q)$  with  $q \geq 5$ ;
- (ii)  $PSL(3, q) \leq G \leq P\Gamma L(3, q)$  with  $q \equiv 3 \pmod{4}$ ;
- (iii)  $PSU(3, q) \leq G \leq PTU(3, q)$  with  $q \equiv 1 \pmod{4}$ ;
- (iv)  $G = \text{Alt}_7$ ;
- (v)  $G = M_{11}$ .

*Proof.* Let  $N$  be a non-abelian simple minimal normal subgroup of  $G$ . We prove that the centralizer  $C_G(N)$  of  $N$  in  $G$  is trivial. Obviously,  $C_G(N) \cap N$  is trivial. If  $C_G(N)$  has an involution  $u$  then  $u \notin N$  and hence a 2-subgroup of  $G$  generated by  $u$  and Sylow 2-subgroup of  $N$  has rank at least 3 contradicting Lemma 6.3. Therefore  $C_G(N)$  has odd order. Then  $C_G(N)$  is trivial, since  $C_G(N)$  is a normal subgroup of  $G$ , and  $G$  is odd core-free. Therefore,  $G$  is isomorphic to an automorphism group of  $N$ . By Lemma 6.7 all possibilities for  $N$  are determined. The cases  $N \cong PSL(2, q)$  with  $q \geq 5$ ,  $N \cong PSL(3, q)$  and  $N \cong PSU(3, q)$  give (i), (ii) and (iii), respectively.

If  $N = \text{Alt}_7$  then either  $G = N$ , or  $G \cong \text{Sym}_7$ . The latter case cannot actually occur as a Sylow 2-subgroup of  $\text{Sym}_7$  has 2-rank 3. Hence (iv) holds. Finally,  $M_{11}$  is isomorphic to its automorphism group, and hence (v) holds.  $\square$

**Remark 6.12.** The subgroups of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$  whose Sylow 2-subgroups have 2-rank 2 are  $PSL(2, q)$ ,  $PGL(2, q)$  and, when  $q = d^h$  with an odd prime  $d$  and  $h \geq 2$ , the semidirect product of  $PSL(2, q)$  or  $PGL(2, q)$  with a cyclic group whose order is an odd divisor of  $h$ . Analog results are valid for  $PSL(3, q)$  and  $PSU(3, q)$ . These groups are all the candidates for  $G$  in (i), (ii), (iii) of Lemma 6.11. It is not true that  $r$  must be equal to  $p$ . For instance, the Hermitian curve of equation  $X^{q+1} + Y^{q+1} + Z^{q+1} = 0$  defined over  $\mathbb{F}_q$  has genus  $\frac{1}{2}q(q-1)$  and if either  $p = 7$  or  $\sqrt{-7} \in \mathbb{F}_q$  it has an automorphism group isomorphic to  $PSL(2, 7)$ .

**Remark 6.13.** The Hermitian curve of equation  $X^6 + Y^6 + 1 = 0$  defined over  $\mathbb{F}_5$  has genus 10 and an automorphism group isomorphic to  $\text{Alt}_7$ . Over an algebraically closed field of characteristic 3, the modular curve  $X(11)$  has genus 26, and its automorphism group is isomorphic to  $M_{11}$ ; see [2, 36].

To apply the above results on any automorphism groups the following lemma is useful.

**Lemma 6.14.** *If a Sylow 2-subgroup of  $G$  fixes no point of  $\mathcal{X}$  then the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  has also even genus.*

*Proof.* If the cover  $\mathcal{X}|\bar{\mathcal{X}}$  is unramified then the claim follows from the Hurwitz genus formula applied to  $O(G)$ . For a point  $\bar{P} \in \bar{\mathcal{X}}$  where  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies, take a point  $P \in \mathcal{X}$  lying over  $\bar{P}$ . Since both  $|O(G)|$  and  $p$  are odd, all ramification groups of  $O(G)_P$  at  $P$  have odd order. From [26, Theorem 11.70],  $d_P$  is even. Let  $\theta$  be the  $G$ -orbit containing  $P$ . Then,  $|G_P||\theta| = |G|$ . Take a Sylow 2-subgroup  $S$  of  $G$  containing a Sylow 2-subgroup  $S_P$  of  $G_P$ . Then  $S \neq S_P$ , as  $S$  does not fix  $P$ . Therefore,  $|S|$  does not divide  $|G_P|$  showing that  $|\theta|$  must be even. This yields that  $d_P|\theta|$  is divisible by four. Since  $O(G)$  is a normal subgroup of  $G$ , [26, Theorem 11.70] implies that  $D(\mathcal{X}|\bar{\mathcal{X}})$  is also divisible by four, that is,  $\frac{1}{2}D(\mathcal{X}|\bar{\mathcal{X}})$  is even. Therefore, the Hurwitz genus formula applied to  $O(G)$  yields  $\mathfrak{g}(\mathcal{X}) - 1 = |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1) + \frac{1}{2}D(\mathcal{X}|\bar{\mathcal{X}})$  whence  $\mathfrak{g}(\bar{\mathcal{X}}) - 1$  is odd.  $\square$

**Remark 6.15.** If a Sylow 2-subgroup of  $G$  is not cyclic, then the hypothesis of Lemma 6.14 is satisfied.

If  $G$  is any subgroup of  $\mathcal{X}$  then the factor group  $G/O(G)$  is an odd core-free automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . If a Sylow 2-subgroup fixes a point of  $\mathcal{X}$  then  $S_2$  is cyclic, and hence  $G = O(G) \rtimes S_2$ . Dismissing this case allows us to use Lemma 6.14. Doing so, either  $\bar{\mathcal{X}}$  is rational and  $\bar{G} = G/O(G)$  is a subgroup of  $PGL(2, \mathbb{K})$ , or  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  and lemmas 6.8 and 6.8 apply. Therefore, the abstract structure of any automorphism group of a curve of even genus can be determined.

**Theorem 6.16.** *For an automorphism group  $G$  of an algebraic curve  $\mathcal{X}$  of even genus  $\mathfrak{g} \geq 2$ , one of the following cases occurs, up to group isomorphisms.*

- (i)  $G$  has odd order.
- (ii)  $G = O(G) \rtimes S_2$  where  $S_2$  is a 2-group described in Remark 6.2.
- (iii) The Sylow 2-subgroups of  $G/O(G)$  are (generalized) quaternion groups, and the commutator subgroup of  $G/O(G)$  is isomorphic to  $SL(2, q)$  with  $q \geq 5$ , apart from two sporadic cases described in Lemma 6.8.
- (iv)  $PSL(2, q) \leq G/O(G) \leq P\Gamma L(2, q)$  with  $q \geq 5$ ;
- (v)  $PSL(3, q) \leq G/O(G) \leq P\Gamma L(3, q)$  with  $q \equiv 3 \pmod{4}$ ;
- (vi)  $PSU(3, q) \leq G/O(G) \leq P\Gamma U(3, q)$  with  $q \equiv 1 \pmod{4}$ ;
- (vii)  $G/O(G) = \text{Alt}_7$ ;
- (viii)  $G/O(G) = M_{11}$ .

## 7. LARGE AUTOMORPHISM GROUPS OF CURVES WITH EVEN GENUS

For large  $|G|$ , refinements of Lemmas 6.11 and 6.8 are obtained.

**Lemma 7.1.** *If  $G$  be an odd core-free group of automorphisms of a curve of even genus  $\mathfrak{g} \geq 2$  such that*

$$(18) \quad |G| > 900\mathfrak{g}^2$$

*then  $\mathcal{X}$  has zero  $p$ -rank, and one of the following three cases occurs for  $G$ , up to group isomorphisms*

- (i)  $PSL(2, q)$ ,  $PGL(2, q)$ ,  $q = p^k \geq 5$ ;
- (ii)  $PSU(3, q)$ ,  $q = p^k$  and  $q \equiv 1 \pmod{4}$ ,  $PGU(3, q)$ ,  $q = p^k$  and  $q \equiv 5 \pmod{12}$ ;
- (iii)  $SL(2, q)$ ,  $SU^\pm(2, q)$ ,  $q \equiv 1 \pmod{4}$ ,  $q = p^k \geq 5$ .

*Proof.* Since  $G$  is odd core-free, its Sylow 2-subgroup is nontrivial and non-cyclic; [28, Chapter I, Aufgaben I.21]. Therefore Lemmas 6.1, 6.4, 6.6, 6.11 and 6.8 apply. As the automorphism group of a genus 2 curve does not exceed 48, our hypothesis (18) rule out (iv) and (v) in Lemma 6.11, as well as (ii) and (iii) in Lemma 6.8. If  $G$  were a 2-group then by Lemma 6.1  $G$  would have a cyclic subgroup of index 2, and hence  $|G| \leq 2(4\mathfrak{g} + 4)$  would hold by [26, Theorem 11.79], a contradiction with (18). If  $G$  has a non-abelian simple normal subgroup then (18) together with Lemmas 6.11, 5.3, and 5.1, and Remark 5.4 show that  $\mathcal{X}$  has

zero  $p$ -rank and that either (i) or (ii) hold. We may assume that a Sylow 2-subgroup of  $G$  is a generalized quaternion group. Then (18) together with Lemma 6.8 show that  $G' \cong SL(2, q)$ . Also,  $\mathcal{X}$  has zero  $p$ -rank by Lemmas 6.10, 5.7, and  $q$  is a power of  $p$  by Lemma 5.7. To prove that case (iii) must occur, consider the factor group  $\bar{G} = G/Z(G)$  which is an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/Z(G)$ . Since the Sylow 2-subgroups of  $G$  are generalized quaternion groups, those of  $\bar{G}$  are dihedral groups. Furthermore, as  $G' \cong SL(2, q)$ ,  $\bar{G}$  has a normal subgroup  $\bar{G}' \cong PSL(2, q)$ . Since  $G$  is odd core-free, the center  $Z(G)$  is a 2-group, and hence  $Z(G)$  is contained in a Sylow 2-subgroup of  $G$ . On the other hand, the center of a generalized quaternion group has order 2. Therefore,  $|Z(G)| = 2$ . Since no two distinct involutions in  $G$  commute, this yields  $Z(G) = Z(G')$ .

First we prove that  $\bar{G}$  is also odd core-free. By absurd, let  $\bar{N}$  be a nontrivial odd order subgroup of  $\bar{G}$ . The subgroup  $N$  of  $G$  containing  $Z(G)$  such that  $N/Z(G) = \bar{N}$  has order a twice an odd number. Hence, its maximal normal subgroup of odd order is nontrivial. Since such a maximal subgroup is a characteristic subgroup of  $N$ , it must be a normal subgroup of  $G$ , a contradiction as  $G$  is odd core-free.

Next we prove that  $\bar{G}$  is isomorphic to a subgroup of  $PGL(2, q)$  containing  $PSL(2, q)$ . Since  $\bar{G}$  is odd core-free and its Sylow 2-subgroups are dihedral, the Gorenstein-Walter theorem applies to  $\bar{G}$  showing that either  $\bar{G} \cong \text{Alt}_7$ , or, up to an isomorphism,  $PSL(2, d) \leq \bar{G} \leq PGL(2, d)$  with an odd prime power  $d \geq 3$ . Since  $PSL(2, d)$  is the commutator subgroup of any subgroup of  $PGL(2, d)$  containing  $PSL(2, d)$ , the claim  $d = q$  follows. The case  $\bar{G} \cong \text{Alt}_7$  does not occur. In fact, from  $2|\text{Alt}_7| = 5040 < 3600 \leq 900\mathfrak{g}(\mathcal{X})^2$ , we would have  $\mathfrak{g}(\mathcal{X}) = 2$ , whereas an hyperelliptic curve has no automorphism group isomorphic to  $\text{Alt}_7$ .

Finally, three cases are distinguished according to the value  $\mathfrak{g}(\bar{\mathcal{X}})$ .

If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  then (18) yields  $|\bar{G}| > 900\mathfrak{g}(\bar{\mathcal{X}})^2$ . From Lemma 5.3 applied to  $\bar{G}$ , either  $\bar{G} = PSL(2, q)$  or  $\bar{G} = PGL(2, q)$ , and  $G/Z_2(G)$  is non-split central extension. In the former case,  $G \cong SL(2, q)$  while in the latter one either  $G \cong SL^\pm(2, q)$  or  $G \cong SU^\pm(2, q)$  according as  $q \equiv -1 \pmod{4}$  or  $q \equiv 1 \pmod{4}$ ; see the proof of [16, Lemma 6.10]. Actually,  $G \cong SL^\pm(2, q)$  cannot occur by Remark 6.5. If  $\mathfrak{g}(\bar{\mathcal{X}}) = 0$ , Lemma 2.1 gives the same possibilities for  $\bar{G}$ , namely  $\bar{G} = PSL(2, q)$  or  $\bar{G} = PGL(2, q)$ , and the same conclusion can be made.

If  $\mathfrak{g}(\bar{\mathcal{X}}) = 1$  then the Hurwitz genus formula shows that the set  $\theta$  of all points fixed by  $Z(G)$  has size  $2\mathfrak{g}(\mathcal{X}) - 2$ . Further,  $\bar{G}$  leaves  $\theta$  invariant. For a point  $\bar{P} \in \theta$ , the stabilizer  $\bar{G}_P$  of  $P$  has order at most 12; see [26, Theorem 11.94]. Therefore,  $|\bar{G}| \leq 12|\theta|$  whence  $|\bar{G}| \leq 24(\mathfrak{g}(\mathcal{X}) - 1)$ . Thus  $|\bar{G}| \leq 48(\mathfrak{g}(\mathcal{X}) - 1)$ . Comparison with (18) shows that this is impossible.  $\square$

**Remark 7.2.** The Hermitian curve of equation  $Y^q + Y = X^{q+1}$  with  $q \equiv 1 \pmod{4}$  is an example for (ii). If  $q \geq 125$ , the Roquette curve  $\mathcal{X}$  of equation  $Y^2 = X^q - X$  provides an example for (iii) with  $G \cong SL(2, q)$  where  $q \equiv 1 \pmod{4}$ .

For the general case, the following result holds.

**Lemma 7.3.** *Let  $G$  be a non-solvable group of automorphisms of a curve of even genus  $\mathfrak{g} \geq 2$  such that (18) holds. Then either  $G/O(G)$  has a non-abelian simple minimal normal subgroup, and one of the following two cases occurs, up to group isomorphisms*

- (A)  $G/O(G) \cong PSL(2, q)$ ,  $G/O(G) \cong PGL(2, q)$ ,  $q = p^k \geq 5$ ;
- (B)  $G/O(G) \cong PSU(3, q)$ ,  $q = p^k$  and  $q \equiv 1 \pmod{4}$ ,  $G/O(G) \cong PGU(3, q)$ ,  $q = p^k$  and  $q \equiv 5 \pmod{12}$ ;

or

- (C)  $G/O(G) \cong SL(2, q)$ ,  $G/O(G) \cong SU^\pm(2, q)$ ,  $q \equiv 1 \pmod{4}$ ,  $q = p^k \geq 5$ .

*Proof.*  $G/O(G)$  is an odd core-free automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ , the assertion follows from Lemma 7.1. From Lemma 6.14,  $\bar{\mathcal{X}}$  is not elliptic. If  $\bar{\mathcal{X}}$  is rational then  $G/O(G)$  is a subgroup of  $PGL(2, q)$  with  $q = p^k$ . Since  $G/(O(G))$  is not solvable, Lemma 2.1 yields that case (A) occurs with only two possible exceptions for  $p \neq 5$  namely  $G/O(G) \cong PSL(2, 5)$  and  $G/O(G) \cong PGL(2, 5)$ .



Both  $PSL(2, 5)$  and  $PGL(2, 5)$  contain a maximal, solvable non-abelian subgroup of index 6. As  $O(G)$  is solvable,  $G$  also has a solvable non-abelian subgroup  $N$  of index 6. This together with (18) give  $|N| > 150\mathfrak{g}^2$ . Since  $N$  is solvable, Theorem 1.1 yields that  $N$  fixes a point  $P \in \mathcal{X}$ . Since  $G$  does not fix  $P$ , and  $N$  is a maximal subgroup of  $G$ , the  $G$ -orbit  $o$  of  $P$  has length 6. By Theorem 1.1,  $\mathcal{X}$  has zero  $p$ -rank. If  $N$  has some elements of order  $p$ , then a  $p$ -subgroup of  $N$  fixes  $P$  and acts transitively on the remaining 5 points in  $o$ . But this yields  $p = 5$ , a contradiction. Otherwise,  $N$  is a prime to  $p$ -subgroup, and the classical Hurwitz bound yields  $|N| < 84(\mathfrak{g} - 1)$  whence  $|G| < 504(\mathfrak{g} - 1)$  contradicting (18).  $\square$

We prove a further result under the hypothesis of Lemma 7.3.

**Lemma 7.4.** *Let  $G$  be a nonsolvable automorphism group of an algebraic curve  $\mathcal{X}$  of even genus  $\mathfrak{g} \geq 2$  such that (18) holds. Then  $\mathcal{X}$  has zero  $p$ -rank. Furthermore,  $O(G)$  is a cyclic prime to  $p$  group, and either  $O(G) = Z(G)$  or  $[Z(G) : O(G)] = 2$  according as cases (A), (B), or (C) in Lemma 7.3 holds.*

*Proof.* We begin with case (A) in Lemma 7.3. We assume that  $G/O(G) \cong PSL(2, q)$  with an odd power  $q \geq 5$  of  $p$ , as the other possibility  $G/O(G) \cong PGL(2, q)$  can be treated analogously. Our first step is to find an upper bound on  $|O(G)|$  in function of  $q$ . Look at  $\bar{G} = G/O(G)$  as an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . This and Lemma 6.14 show that either  $\bar{\mathcal{X}}$  is rational, or  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ . In the latter case, since  $\bar{G}$  contains an abelian subgroup of order  $q$ , [26, Theorem 11.79] yields  $4\mathfrak{g}(\bar{\mathcal{X}}) + 3 \geq q$  whence  $4\mathfrak{g}(\bar{\mathcal{X}}) + 4 \geq q + 1$ .

If  $\bar{\mathcal{X}}$  is not rational, the Hurwitz genus formula applied to  $O(G)$  gives  $\mathfrak{g} - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ . From  $|PSL(2, q)||O(G)| = |G| > 900\mathfrak{g}^2$ ,

$$(19) \quad \frac{\frac{1}{2}(q-1)q}{|O(G)|(q+1)} > 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{q+1} \right)^2 > 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{4(\mathfrak{g}(\bar{\mathcal{X}}) + 1)} \right)^2 > \frac{900}{144} = \frac{25}{4}.$$

This also shows that

$$(20) \quad |O(G)| < q,$$

and that  $q > 11$ .

If  $\bar{\mathcal{X}}$  is rational, then  $\bar{G}$  acts on  $\bar{\mathcal{X}}$  as  $PSL(2, q)$  on the projective line  $PG(1, \mathbb{K})$ . Take any point  $\bar{P} \in \bar{\mathcal{X}}$ . As  $PSL(2, q)$  is not solvable,  $\bar{G}$  does not fix  $\bar{P}$ . Hence, the  $\bar{G}$ -orbit of  $\bar{P}$  has length at least  $q$ . In fact,  $|\bar{G}_{\bar{P}}| \leq \frac{1}{2}q(q-1)$  as the order of the largest proper subgroup of  $PSL(2, q)$  is  $\frac{1}{2}q(q-1)$ . This follows from [26, Theorem 11.74] and Lemma 2.1. Now take a point  $P \in \mathcal{X}$  where the cover  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies. Then the  $G$ -orbit  $o$  of  $P$  has length at least  $qu$  where  $u = |O(G)|/|O(G)_P|$ . The Hurwitz genus formula applied to  $O(G)$  yields

$$2\mathfrak{g} - 2 \geq -2|O(G)| + |o|(|O(G)_P| - 1) \geq -2|O(G)| + |o|\frac{2}{3}|O(G)_P| \geq |O(G)|(\frac{2}{3}q - 2).$$

Hence  $\mathfrak{g} > \frac{1}{3}(q-3)|O(G)|$ . From this and  $\frac{1}{2}(q+1)q(q-1)|O(G)| > 900\mathfrak{g}^2$ ,

$$|O(G)| < \frac{9}{2 \cdot 900} \frac{(q+1)(q-1)}{(q-3)^2} q < \frac{9 \cdot 6 \cdot 4}{8 \cdot 900} q = \frac{3}{100} q < q,$$

whence  $q > 100$  follows.

Therefore, both (19) and (20) are true for any  $\bar{\mathcal{X}}$ . Also,  $q > 11$  must hold.

Assume that  $\bar{\mathcal{X}}$  is not rational. Since  $\bar{G} \cong PSL(2, q)$ ,  $\bar{\mathcal{X}}$  cannot be a genus 2 curve; see [41, Theorem 2]. Then  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 3$  and hence

$$(21) \quad \mathfrak{g} > \mathfrak{g} - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1) > \frac{2}{3}|O(G)|\mathfrak{g}(\bar{\mathcal{X}}).$$

This shows that  $|G| = \frac{1}{2}q(q-1)(q+1)|O(G)| > 900\mathfrak{g}^2$  yields

$$|\bar{G}| = \frac{1}{2}q(q-1)(q+1) > 900\mathfrak{g}(\bar{\mathcal{X}})^2.$$

From Lemma 7.1 applied to  $\bar{G}$ , the  $p$ -rank of  $\bar{\mathcal{X}}$  is equal to zero. Obviously this remains true when  $\bar{\mathcal{X}}$  is rational.



Therefore, a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{G} \cong PSL(2, q)$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . Here  $|Q| = p^k$ , and the normalizer of  $\bar{Q}$  in  $\bar{G}$  is the semidirect product  $\bar{Q} \rtimes \bar{T}$  with a cyclic group  $\bar{T}$  of order  $\frac{1}{2}(q-1)$ . Since this normalizer is a maximal subgroup of  $\bar{G}$ , it is the stabilizer of  $\bar{P}$  in  $\bar{G}$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . The counter-image of  $\bar{Q} \rtimes \bar{T}$  in the homomorphism  $G \mapsto \bar{G}$  is a subgroup  $N$  of order  $\frac{1}{2}(q-1)q|O(G)|$  where  $N$  is the subgroup of  $G$  which preserves  $o$ . For a point  $P \in o$ , the stabilizer  $H$  of  $P$  in  $N$  has order  $\frac{1}{2}(q-1)q|O(G)_P|$ . Therefore, the (unique) Sylow  $p$ -subgroup  $Q_1$  of  $H$  has order  $q_1 = qp^a$  and a complement of  $Q_1$  in  $H$  is a cyclic subgroup  $C_t$  of order  $t = \frac{1}{2}(q-1)b$  with  $p \nmid b$ . Hence  $H = Q_1 \rtimes C_t$ , and  $|o|p^ab = |O(G)|$ . Now, since  $|G| = \frac{1}{2}q(q-1)(q+1)|O(G)| > 900\mathfrak{g}^2$  yields  $\frac{1}{2}q(q-1)p^ab(q+1)|o| > 900\mathfrak{g}^2$ , (19) gives

$$|H|^2 = (q_1t)^2 > \frac{\frac{1}{2}(q-1)qp^ab}{(q+1)|o|}900\mathfrak{g}^2 = (p^ab)^2 \frac{\frac{1}{2}(q-1)q}{|O(G)|(q+1)}900\mathfrak{g}^2 > 900\mathfrak{g}^2$$

whence

$$|H| = q_1t > 30\mathfrak{g}.$$

From Lemma 4.1 and Remark (4.3), either  $\mathcal{X}$  has zero  $p$ -rank, or  $Q_1$  has just one short orbit  $\theta$  other than its fixed point  $P$ . Observe that  $\theta$  is contained in  $o$ . In fact, each  $Q_1$ -orbit in  $o$  is short as  $|o| \leq |O(G)| < q < q_1$  by (20). Therefore  $o = \theta \cup \{P\}$ , and hence  $|o| = 1 + p^h$  for some  $h \geq 0$ . Since  $|o|$  divides  $|O(G)|$  this implies that  $|O(G)|$  is even, a contradiction. Thus  $\mathcal{X}$  has zero  $p$ -rank.

To complete our investigation of case (A) in Lemma 7.1, we show that  $O(G)$  is a prime to  $p$  cyclic group, and that  $Z(G) = O(G)$ . For every  $h \in G$  the map  $\varphi_h$  taking  $u \in O(G)$  to  $h^{-1}uh$  is an automorphism of  $O(G)$ , and hence the map  $\Phi : h \mapsto \varphi_h$  is a homomorphism from  $G$  into  $\text{Aut}(O(G))$ . Take a Sylow  $p$ -subgroup  $Q$  of  $G$ . Since  $\mathcal{X}$  has zero  $p$ -rank, [26, Theorem 11.129] yields that  $Q$  fixes a unique point  $P \in \mathcal{X}$  but no nontrivial element of  $Q$  fixes a point other than  $P$ . If  $g$  is any element in  $O(G)$ , then (20) yields that the  $Q$ -orbit of  $g$  in the action of  $\Phi$  has length smaller than  $q$ . Hence,  $g$  commutes with a non-trivial element of  $Q$ . Therefore,  $g$  fixes  $P$ , and hence  $O(G)$  does, as well. Repeating this argument with another Sylow  $p$ -subgroup of  $G$ , it turns out that  $O(G)$  fixes point  $P' \in \mathcal{X}$  other than  $P$ . From (i) of Lemma 3.1,  $O(G)$  contains no element of order  $p$ . Therefore  $O(G)$  is a cyclic prime to  $p$  group. In particular,  $O(G) \leq \ker(\Phi)$ . We show that  $\ker(\Phi) = G$ . By absurd,  $O(G) = \ker(\Phi)$  as  $G/O(G)$  is a simple group, and  $\ker(\Phi)$  is a normal subgroup of  $G$ . Hence  $\Phi$  induces a faithful action of  $PSL(2, q) \cong G/O(G)$  on  $O(G)$ . If  $\Lambda$  is a nontrivial orbit then  $|\Lambda| < q$  by (20). On the other hand,  $|\Lambda|$  is at least as large as the index of the largest subgroup of  $PSL(2, q)$ . Since  $q > 11$ , the largest subgroup of  $PSL(2, q)$  has order  $\frac{1}{2}q(q-1)$ , see [26, Theorem A.8]. Therefore, its index is  $q+1$ , and hence  $|\Lambda| \geq q+1$ , a contradiction. Therefore,  $\ker(\Phi) = G$  and hence  $Z(G) = O(G)$ .

We continue with case (B) in Lemma 7.3. We assume that  $G/O(G) \cong PSU(3, q)$  with a power  $q \equiv 1 \pmod{4}$  of  $p$  as the other possibility  $G/O(G) \cong PGU(3, q)$  can be treated analogously. Then

$$(22) \quad (q^2 - 1)q^3(q^3 + 1)|O(G)| > 900\mathfrak{g}^2.$$

The quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  is not rational as  $\bar{G} = G/O(G)$  is an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  but  $PGL(2, \mathbb{K})$  has no subgroup isomorphic to  $\bar{G} \cong PSU(3, q)$ . Also,  $\bar{\mathcal{X}}$  is neither elliptic by Lemma 6.14.

First we show how the above proof for case (A) can be adapted to deal with case (B) under the hypothesis

$$(23) \quad \frac{(q^2 - 1)q^3}{|O(G)|(q^3 + 1)} > 1.$$

From Lemma 7.1 applied to  $\bar{G}$ , the  $p$ -rank of  $\bar{\mathcal{X}}$  is equal to zero. Therefore, a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{G}$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . This time,  $|Q| = p^k$  and the normalizer of  $\bar{Q}$  in  $\bar{G}$  is the semidirect product  $\bar{Q} \rtimes \bar{T}$  where  $\bar{Q}$  is a non-abelian  $p$ -group of order  $q^3$  while  $\bar{T}$  is a cyclic group of order  $q^2 - 1$ . Since this normalizer is a maximal subgroup of  $\bar{G}$ , it is the stabilizer of  $\bar{P}$  in  $\bar{G}$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . The counter-image of  $\bar{Q} \rtimes \bar{T}$  in the homomorphism  $G \mapsto \bar{G}$  is a subgroup  $N$  of order

$(q^2 - 1)q^3|O(G)|$ . For a point  $P \in o$ , the stabilizer of  $P$  in  $N$  is a subgroup  $H$  of order  $(q^2 - 1)q^3|O(G)_P|$ . Therefore, the (unique) Sylow  $p$ -subgroup  $Q_1$  of  $H$  has order  $q_1 = q^3p^a$  and a complement of  $Q_1$  in  $H$  is a cyclic subgroup  $C_t$  of order  $t = (q^2 - 1)b$  with  $p \nmid b$ . Hence  $H = Q_1 \rtimes C_t$ , and  $|o|p^ab = |O(G)|$ . Now, since  $|G| = q^3(q^2 - 1)(q^3 + 1)|O(G)| > 900\mathfrak{g}^2$  means  $(q^2 - 1)q^3p^ab(q^3 + 1)|o| > 900\mathfrak{g}^2$ , (23) gives

$$|H|^2 = (q_1t)^2 > \frac{(q^2 - 1)q^3p^ab}{(q^3 + 1)|o|} 900\mathfrak{g}^2 = (p^ab)^2 \frac{(q^2 - 1)q^3}{|O(G)|(q^3 + 1)} 900\mathfrak{g}^2 > 900\mathfrak{g}^2$$

whence

$$|H| > 30\mathfrak{g}.$$

From Lemma 4.1 and Remark (4.3), either  $\mathcal{X}$  has zero  $p$ -rank, or  $Q_1$  has just one short orbit  $\theta$  other than its fixed point  $P$ . Observe that  $\theta$  is contained in  $o$ . In fact, each  $Q_1$ -orbit in  $o$  is short as  $|o| \leq |O(G)| < q^2 < q^3 < q_1$  by (24). Therefore  $o = \theta \cup \{P\}$ , and hence  $|o| = 1 + p^h$  for some  $h \geq 0$ . Since  $|o|$  divides  $|O(G)|$  this implies that  $|O(G)|$  is even, a contradiction. Thus  $\mathcal{X}$  has zero  $p$ -rank. Furthermore, under the stronger hypothesis

$$(24) \quad \frac{(q^2 - 1)q^3}{|O(G)|(q^3 + 1)} > \left(\frac{75}{8}\right)^2 > 87.$$

$O(G) = Z(G)$  and  $O(G)$  is a cyclic prime to  $p$  group. This can be shown by the argument used in case (A), as (22) implies  $|Q| < q^3$ , and the largest subgroup of  $PSU(3, q)$  has order  $q^3(q^2 - 1)/\mu$ ; see [26, Theorem A.10] and [33].

Next we show that (24) holds if the cover  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies. Take a ramification point  $\bar{P} \in \bar{\mathcal{X}}$ . Since  $PSU(3, q)$  is simple,  $\bar{G}$  does not fix  $\bar{P}$ . Let  $\bar{o}$  be the  $\bar{G}$ -orbit of  $\bar{P}$ . From the classification of subgroups of  $PSU(3, q)$ , the maximum order of a proper subgroup of  $\bar{G}$  is  $q^3(q^2 - 1)/\mu$ . From this,  $|\bar{o}| \geq q^3 + 1$ . Therefore, the cover  $\mathcal{X}|\bar{\mathcal{X}}$  has at least  $q^3 + 1$  ramification points with the same ramification index. If the  $O(G)$ -orbit lying over  $\bar{P}$  has length  $\ell$ ,

$$2\bar{\mathfrak{g}} - 2 \geq -2|O(G)| + (q^3 + 1)(|O(G)| - \ell) \geq |O(G)|\left(\frac{2}{3}(q^3 + 1) - 2\right) > |O(G)|\frac{5}{8}(q^3 + 1),$$

whence

$$\mathfrak{g} > \bar{\mathfrak{g}} - 1 > \frac{5}{16}(q^3 + 1)|O(G)|.$$

This together with (22) give (24).

Therefore we are left with the case where the cover  $\mathcal{X}|\bar{\mathcal{X}}$  is unramified. As  $\mathfrak{g}$  is even  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 4$ , and from (22),

$$(25) \quad |\bar{G}| > 900|O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)^2 \geq \frac{8100}{16}|O(G)|\mathfrak{g}(\bar{\mathcal{X}})^2 \geq \frac{27}{16} \cdot 900\mathfrak{g}(\bar{\mathcal{X}})^2.$$

By absurd,  $\mathcal{X}$  is assumed to be a minimal counter-example.

Assume that  $O(G)$  has a proper normal subgroup  $N$ . Suppose that  $N$  is also a normal subgroup of  $G$ , and consider the quotient curve  $\tilde{\mathcal{X}} = \mathcal{X}/N$ . From  $N \leq O(G)$ , we have  $\mathfrak{g}(\tilde{\mathcal{X}}) \geq \mathfrak{g}(\bar{\mathcal{X}}) \geq 4$ . From the Hurwitz genus formula applied to  $N$ ,

$$\mathfrak{g} > \mathfrak{g} - 1 = |N|(\mathfrak{g}(\tilde{\mathcal{X}}) - 1) \geq \frac{3}{4}|N|\mathfrak{g}(\tilde{\mathcal{X}}).$$

Since  $\tilde{G} = G/N$  is a subgroup of  $\text{Aut}(\tilde{\mathcal{X}})$ , and  $|N| \geq 3$ ,

$$|\tilde{G}| > 900|N|(\mathfrak{g}(\tilde{\mathcal{X}}) - 1)^2 \geq \frac{8100}{16}|N|\mathfrak{g}(\tilde{\mathcal{X}})^2 \geq \frac{27}{16} \cdot 900\mathfrak{g}(\tilde{\mathcal{X}})^2.$$

Note that  $\tilde{G}$  is a nonsolvable group and that the factor group  $O(G)/N$  is the largest normal subgroup  $O(\tilde{G})$  of  $\tilde{G}$  of odd order. Also, the cover  $\tilde{\mathcal{X}}|(\tilde{\mathcal{X}}/O(\tilde{G}))$  is unramified. As  $\mathcal{X}$  was assumed to be a minimal counter-example,  $\tilde{\mathcal{X}}$  has zero  $p$ -rank. Let  $\tilde{S}_p$  a Sylow  $p$ -subgroup of  $\tilde{G}$ . Then  $\tilde{S}_p$  fixes a unique point  $\tilde{P} \in \tilde{\mathcal{X}}$ . Since the cover  $\tilde{\mathcal{X}}|\bar{\mathcal{X}}$  is unramified, no nontrivial element of  $O(\tilde{G})$  fixes a point of  $\tilde{\mathcal{X}}$ . Therefore,  $\tilde{S}_p \cap O(\tilde{G})$  is trivial, and  $p \nmid O(\tilde{G})$ . Let  $\tilde{M}$  be the subgroup of  $\tilde{G}$  generated by  $\tilde{S}_p$  together with  $O(\tilde{G})$ . Then  $\tilde{M}$  is the

semidirect product  $\tilde{S}_p \rtimes O(\tilde{G})$ . Observe that  $\tilde{S}_p$  is not a normal subgroup of  $\tilde{M}$  as  $\tilde{M}$  does not fix  $\tilde{P}$ . From the Burnside-Gow theorem [26, Theorem 11.334],  $\tilde{S}_p$  is cyclic. On the other hand,  $\tilde{S}_p$  is isomorphic to a Sylow  $p$ -subgroup of  $PSU(3, q)$ . But this contradicts the fact that the Sylow  $p$ -subgroups of  $PSU(3, q)$  are not cyclic. Therefore,  $O(G)$  contains no proper normal subgroup of  $G$ .

In particular,  $O(G)$  is characteristically simple, and hence  $O(G) = C_d \times \cdots \times C_d$  with a cyclic group  $C$  of odd prime order  $d$ ; see [28, Section I, Theorem 9.2].

First the case  $d \neq p$  is investigated. As in case (A), let  $\Phi$  denote the homomorphism from  $G$  to the automorphism group of  $O(G)$  arising from conjugacy. Assume that  $\ker(\Phi)$  contains  $O(G)$  properly. Then  $\ker(\Phi)/O(G)$  is a nontrivial normal subgroup of  $\bar{G}$ . Since  $\bar{G} \cong PSU(3, q)$  is a simple group, this only happens when  $\ker(\Phi)/O(G) = \bar{G}$ . Therefore  $\ker(\Phi) = G$  whence  $Z(G) = O(G)$ . Thus  $G/Z(G) \cong PSU(3, q)$ .

If the commutator subgroup  $G'$  of  $G$  does not contain  $O(G)$  then they intersect trivially as  $O(G)$  contains no proper normal subgroup of  $G$ . Therefore,  $G' \times O(G)$  is a subgroup of  $G$ . Since  $G/O(G) \cong PSU(3, q)$ , this implies  $G' \cong PSU(3, q)$ , and hence  $G = G' \times O(G)$  with  $G' \cong PSU(3, q)$ . Take a point  $\bar{P} \in \bar{\mathcal{X}}$  fixed by a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{G}$ . The  $O(G)$ -orbit  $o$  lying over  $\bar{P}$  is left invariant by a subgroup  $Q$  of  $G$  such that  $Q/O(G) = \bar{Q}$ . Since  $|O(G)|$  is prime to  $|\bar{Q}| = q^3$ , we have  $Q = O(G) \times Q'$  where  $|Q'| = |\bar{Q}|$ , and  $Q'$  fixes a point  $P \in o$ . Since  $Z(G) = O(G)$ , this yields that  $Q'$  fixes  $o$  pointwise. From the Deuring-Shafarevich formula applied to  $Q'$ ,

$$\gamma(\mathcal{X}) - 1 \geq -q^3 + |O(G)|(q^3 - 1)$$

Taking into account that  $\mathfrak{g} \geq \gamma(\mathcal{X})$ , a straightforward computation yields (24), and hence  $\mathcal{X}$  has zero  $p$ -rank.

If the commutator subgroup  $G'$  contains  $O(G) = Z(G)$ , then  $G/Z(G) \cong PSU(3, q)$  shows that  $G$  is a covering group of  $PSU(3, q)$ . From [21, Theorem 2], the unique maximal covering group of  $PSU(3, q)$  is  $SU(3, q)$ , and hence  $G$  is a subgroup of  $SU(3, q)$ . Since  $Z(G)$  is nontrivial, it turns out that  $G$  is a subgroup of  $SU(3, q)$  with  $q + 1 \equiv 0 \pmod{3}$ . Thus  $|Z(G)| = |O(G)| = 3$  and (23) holds. Hence,  $\mathcal{X}$  has zero  $p$ -rank.

Therefore  $\ker(\Phi) = O(G)$  is assumed. Then  $G/O(G) \cong PSU(3, q)$  has a faithful representation  $\Phi$  by a matrix group of the vector space  $V(r, d)$  where  $|O(G)| = d^r$ . Since no nontrivial normal subgroup of  $G$  is contained in  $O(G)$ ,  $\Phi$  is irreducible. Let  $PG(r - 1, d)$  be the projective space arising from  $V(r, d)$ . Since  $PSU(3, q)$  is simple, we also have an irreducible, faithful representation of  $PSU(3, q)$  as a projective group of  $PG(r - 1, d)$ . Since  $d \neq p$ , this yields  $r - 1 \geq q(q - 1)$ ; see [29]. Hence  $|O(G)| > d^{q(q-1)+1}$ . But this contradicts (25).

Finally, the case  $p = d$  is investigated. By (25), together with Lemma 5.1,  $\bar{\mathcal{X}}$  has zero  $p$ -rank. Let  $\bar{Q}$  be a Sylow  $p$ -subgroup of  $\bar{G}$ . Since  $\bar{\mathcal{X}}$  has zero  $p$ -rank, there is a point  $\bar{P} \in \bar{\mathcal{X}}$  which is fixed by  $\bar{Q}$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G$  containing  $O(G)$  such that  $\bar{Q} = Q/O(G)$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $|o| = |O(G)|$ , for each  $P \in o$  the stabilizer of  $P$  in  $Q$  has order  $q^3$ ; on the other hand,  $Q$  acts semiregularly on  $\mathcal{X} \setminus o$ . From the Deuring-Shafarevich formula applied to  $Q$ ,

$$\gamma(\mathcal{X}) - 1 = -|Q| + |O(G)|(q^3 - 1) = -|O(G)|,$$

a contradiction.

Case (C) in Lemma 7.3 can be worked out using the argument employed for case (A). Let  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  and  $\bar{G} = G/O(G)$ . We assume that  $G/O(G) \cong SL(2, q)$  with an odd power  $q \geq 5$  of  $p$ , as the other possibilities  $G/O(G) = SU^\pm(2, q)$ ,  $q \equiv 1 \pmod{4}$  can be treated analogously.

As  $\bar{G} \cong SL(2, q)$  and  $PGL(2, \mathbb{K})$  contains no subgroup isomorphic to  $SL(2, q)$ ,  $\bar{\mathcal{X}}$  is not rational. Furthermore, since a Sylow 2-subgroup of  $SL(2, q)$  is not cyclic, Lemma 6.14 and Remark 6.2 yield that  $\bar{\mathcal{X}}$  is neither elliptic. Therefore,  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ . Also,  $\mathfrak{g} - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$  by the Hurwitz genus formula applied to  $O(G)$ . From  $(q - 1)q(q + 1)|O(G)| = |SL(2, q)||O(G)| = |G| > 900\mathfrak{g}^2$ ,

$$(26) \quad \frac{(q - 1)q}{|O(G)|(q + 1)} > 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{q + 1} \right)^2 > 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{4(\mathfrak{g}(\bar{\mathcal{X}}) + 1)} \right)^2 \geq \frac{900}{144} = \frac{25}{4}.$$

From this,

$$(27) \quad |O(G)| < \frac{1}{2}q,$$

and  $q > 11$  follow. As in case (A), this yields that  $\bar{\mathcal{X}}$  cannot be a genus 2 curve and hence (21) holds; therefore,

$$|\bar{G}| = q(q-1)(q+1) > 900\mathbf{g}(\bar{\mathcal{X}})^2.$$

By Lemma 7.1,  $\bar{\mathcal{X}}$  has zero  $p$ -rank. Therefore, a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{G}' \cong SL(2, q)$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . Here  $|\bar{Q}| = q$ , and the normalizer of  $\bar{Q}$  in  $\bar{G}'$  is the semidirect product  $\bar{Q} \rtimes \bar{T}$  with a cyclic group  $\bar{T}$  of order  $q-1$ . Since this normalizer is a maximal subgroup of  $\bar{G}'$ , it is the stabilizer of  $\bar{P}$  in  $\bar{G}'$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . The counter-image of  $\bar{Q} \rtimes \bar{T}$  in the homomorphism  $G \mapsto \bar{G}$  is a subgroup  $N$  of order  $(q-1)q|O(G)|$  where  $N$  is the subgroup of  $G$  which preserves  $o$ . For a point  $P \in o$ , the stabilizer  $H$  of  $P$  in  $N$  has order  $(q-1)q|O(G)_P|$ . Therefore, the (unique) Sylow  $p$ -subgroup  $Q_1$  of  $H$  has order  $q_1 = qp^a$  and a complement of  $Q_1$  in  $H$  is a cyclic subgroup  $C_t$  of order  $t = (q-1)b$  with  $p \nmid b$ . Hence  $H = Q_1 \rtimes C_t$ , and  $|o|p^ab = |O(G)|$ . Now, since  $|G| = q(q-1)(q+1)|O(G)| > 900\mathbf{g}^2$  yields  $q(q-1)p^ab(q+1)|o| > 900\mathbf{g}^2$ , (26) gives

$$|H|^2 = (q_1t)^2 > \frac{(q-1)qp^ab}{(q+1)|o|}900\mathbf{g}^2 = (p^ab)^2 \frac{(q-1)q}{|O(G)|(q+1)}900\mathbf{g}^2 > 900\mathbf{g}^2,$$

whence

$$|H| = q_1t > 30\mathbf{g}.$$

From Lemma 4.1 and Remark (4.3), either  $\mathcal{X}$  has zero  $p$ -rank, or  $Q_1$  has just one short orbit  $\theta$  other than its fixed point  $P$ . Observe that  $\theta$  is contained in  $o$ . In fact, each  $Q_1$ -orbit in  $o$  is short as  $|o| \leq |O(G)| < q < q_1$  by (20). Therefore  $o = \theta \cup \{P\}$ , and hence  $|o| = 1 + p^h$  for some  $h \geq 0$ . Since  $|o|$  divides  $|O(G)|$  this implies that  $|O(G)|$  is even, a contradiction. Thus  $\mathcal{X}$  has zero  $p$ -rank.

Finally, the argument for case (A) is adapted to show that  $Z(G)$  is a cyclic prime to  $p$  group containing  $O(G)$  as an index 2 subgroup. For this purpose, let  $M$  be the normal subgroup of  $G$  containing  $O(G)$  such that  $M/O(G) = Z(G/O(G))$ . Since  $G/O(G) \cong SL(2, q)$ ,  $Z(G/O(G))$  has order two, and hence  $|M| = 2|O(G)|$ . For every  $h \in G$  the map  $\varphi_h$  taking  $u \in M$  to  $h^{-1}uh$  is an automorphism of  $M$ , and hence the map  $\Phi : h \mapsto \varphi_h$  is a homomorphism from  $G$  into  $\text{Aut}(O(G))$ . Now, after replacing  $O(G)$  by  $M$ , the argument for case (A) can be used to prove that  $M$  is a cyclic prime to  $p$  group. In particular,  $M \leq \ker(\Phi)$ . We show that  $\ker(\Phi) = G$ . By absurd,  $M = \ker(\Phi)$  as  $G/M \cong PSL(2, q)$  is a simple group, and  $\ker(\Phi)$  is a normal subgroup of  $G$ . Hence  $\Phi$  induces a faithful action of  $PSL(2, q)$  on  $M$ . If  $\Lambda$  is a nontrivial orbit then  $|\Lambda| < q$  by (27). On the other hand,  $|\Lambda| \geq q+1$  by the argument used for case (A). This contradiction shows that  $\ker(\Phi) = G$  whence  $Z(G) = M$ .  $\square$

## 8. PROOF OF THEOREM 1.2

Both Lemmas 7.3 and 7.4 hold. In particular,  $\mathcal{X}$  has zero  $p$ -rank,  $O(G)$  is cyclic and  $O(G) \leq Z(G)$ .

If  $O(G) = \{1\}$ , Theorem 1.2 follows from Lemma 7.1. Therefore,  $O(G)$  is assumed to be non-trivial.

From (i) of Lemma 3.1, every Sylow  $p$ -subgroup fixes a point of  $\mathcal{X}$ . Let  $o$  denote the set of all such points. Then there is a bijection between  $\Omega$  and the set of all Sylow  $p$ -subgroups of  $G$ . Since the Sylow  $p$ -subgroups of  $G$  are conjugated in  $G$ ,  $o$  is a  $G$ -orbit. Therefore,  $G$  has a transitive permutation representation  $\Phi$  on  $\Omega$ . Let  $\tilde{G} = G/\ker(\Phi)$ . Then  $Z(G) \leq \ker(\Phi)$  as  $Z(G)$  fixes  $\Omega$  pointwise. Furthermore,  $Z(G)$  is a prime to  $p$  subgroup, and hence  $G/Z(G)$  is divisible by  $p$ .

If case (A) or (B) in Lemma 7.3 holds, then  $G/Z(G)$  is either a simple group or it has only one normal subgroup, and in the latter case the index of the normal subgroup in  $G$  is prime to  $p$ . This implies that  $\ker(\Phi) = O(G) = Z(G)$ . Therefore,  $\tilde{G}$  acts (by conjugation) on  $\Omega$  faithfully in the same way as either  $PSL(2, q)$ , or  $PGL(2, q)$ , or  $PSU(3, q)$ , or  $PGU(3, q)$ , on the set of their Sylow  $p$ -subgroups, that is, in their

usual doubly transitive permutation representation. In particular,  $q = |\Omega| - 1$  for  $PSL(2, q)$  and  $PGL(2, q)$  while  $q^3 = |\Omega| - 1$  for  $PSU(3, q)$  and  $PGU(3, q)$ .

If case (C) in Lemma 7.3 occurs, then  $[Z(G) : O(G)] = 2$  and either  $G/Z(G) \cong PSL(2, q)$ , or  $G/Z(G) \cong PGL(2, q)$ . In the former case,  $G/Z(G)$  is simple, in the latter one  $G/Z(G)$  has unique normal subgroup whose index is 2, and hence prime to  $p$ . Therefore,  $\ker(\Phi) = Z(G)$ , and  $\tilde{G}$  acts on  $\Omega$  faithfully as either  $PSL(2, q)$ , or  $PGL(2, q)$ , on the set of their Sylow  $p$ -subgroups, that is, in their usual doubly transitive permutation representation.

Let  $S_p$  be a Sylow  $p$ -subgroup of  $G$ , and look at the action of  $S_p$  on  $\Omega$ . Obviously  $S_p$  fixes the point  $P \in \Omega$  represented by  $S_p$  itself. From (i) of Lemma 3.1, no nontrivial element of  $S_p$  fixes another point, that is,  $S_p$  acts semiregularly on the points of  $\Omega$  other than  $P$ . Actually,  $S_p$  is regular on  $\Omega \setminus \{P\}$ . Furthermore,  $S_p$  is a normal subgroup of the stabilizer of  $P$  in  $G$ .

Therefore, the pair  $(\Omega, G)$  is a group space satisfying the hypothesis of Hering's theorem, [27, Theorem 2.4], where  $Q = S_p$ , and the normal closure  $S$  of  $Q$  is the subgroup  $p(G)$  of  $G$  generated by all Sylow  $p$ -subgroups of  $G$ . In Hering's theorem, there are several possibilities for  $S$  and hence for our  $p(G)$ , but those consistent with Lemma 7.3 are only four, namely  $PSL(2, q)$ ,  $SL(2, q)$ ,  $PSU(3, q)$  with  $q \equiv 1 \pmod{4}$  and  $SU(3, q)$  with  $q \equiv 5 \pmod{12}$ . This completes the proof of Theorem 1.2.

## 9. EXAMPLES FOR THEOREM 1.2

In Remark 7.2 we have already pointed out that Hermitian curves and Roquette curves provide example for the cases  $p(G) = PSU(3, q)$ ,  $PGL(2, q)$ ,  $SL(2, q)$ .

We show that the Hermitian curve and the GK-curve have quotient curves that provide examples for Theorem 1.2.

Let  $q$  be a power of  $p$  such that  $q \equiv 1 \pmod{4}$ .

The Hermitian curve  $\mathcal{Y}$  has even genus  $g(\mathcal{Y}) = \frac{1}{2}q(q-1)$ . Up to an isomorphism,  $\text{Aut}(\mathcal{Y}) = PGU(3, q)$  and  $p(\text{Aut}(\mathcal{Y})) = PSU(3, q)$  as in the first case in Theorem 1.2.

Take  $\mathcal{Y}$  with its homogeneous equation  $X^{q+1} + Y^{q+1} + Z^{q+1} = 0$ . Let  $T = \langle t \rangle$  be the subgroup of  $PGU(3, q)$  generated by  $t : (X, Y, Z) \rightarrow (wX, wY, Z)$  where  $w \in \mathbb{K}$  has order  $m$  for some divisor  $m$  of  $q+1$ . Here  $t$  (and every nontrivial element of  $T$ ) fixes exactly  $q+1$  points of  $\mathcal{Y}$ , those lying on the line of equation  $Z = 0$  at infinity. From the Hurwitz genus formula, the quotient curve  $\mathcal{X}_m = \mathcal{Y}/T$  has even genus  $g(\mathcal{X}_m) = \frac{1}{2}((q-1-m)(q+1)/m+2)$ , and  $G = PGU(3, q)$  is a subgroup of  $\text{Aut}(\mathcal{X}_m)$ . If  $m$  is even then  $G \cong PGL(2, q) \times C_{(q+1)/m}$  while for odd  $m$ ,  $G \cong SU(2, q)^\pm \times C_{(q+1)/2m}$ . An index 2 subgroup of  $G$  is isomorphic to  $PSL(2, q) \times C_{(q+1)/2}$  for  $m$  even and to  $SL(2, q) \times C_{(q+1)/2m}$  for  $m$  odd. In all cases,  $|G| > 900g(\mathcal{X})^2$  for  $m$  big enough, namely  $m > 225$ , and examples for  $p(G) \cong PSL(2, q)$ ,  $PGL(2, q)$ ,  $SL(2, q)$  in Theorem 1.2 are obtained.

The GK-curve  $\mathcal{Z}$  has even genus  $g(\mathcal{Z}) = \frac{1}{2}(q^3+1)(q^2-2)+1$  and  $\text{Aut}(\mathcal{Z})$  has order  $(q^3+1)q^3(q^2-1)(q^2-q+1)$ . More precisely,  $\text{Aut}(\mathcal{Z}) \cong PSU(3, q) \times C_{q^2-q+1}$  for  $q \not\equiv -1 \pmod{3}$  while  $\text{Aut}(\mathcal{Z})$  has an index 3 subgroup  $G \cong SU(3, q) \times C_{(q^2-q+1)/3}$  for  $q \equiv -1 \pmod{3}$ ; see [11]. In particular,  $|\text{Aut}(\mathcal{Z})| \approx 8g(\mathcal{X})^2$ . Furthermore,  $\text{Aut}(\mathcal{Z})$  has exactly two short orbits. One of them has size  $q^3+1$  and the kernel of the permutation representation of  $\text{Aut}(\mathcal{Z})$  on it is the cyclic subgroup  $C_{q^2-q+1}$  of  $\text{Aut}(\mathcal{Z})$  while no nontrivial element of  $C_{q^2-q+1}$  fixes a point in the other short orbit. The quotient curves of  $\mathcal{Z}$  are thoroughly investigated in [10]

Here we limit ourselves to a special case, also discussed in [11].

For a divisor  $d$  of  $q^2 - q + 1$ , the group  $C_{q^2-q+1}$  contains a subgroup  $C_d$  of order  $d$ . Let  $\mathcal{X}_d = \mathcal{Z}/C_d$  the quotient curve of  $\mathcal{X}$  with respect to  $C_d$ . Since  $C_d$  is tame, the Hurwitz genus formula gives

$$(q^3+1)(q^2-2) = 2g(\mathcal{Y}) - 2 = d(2g(\mathcal{X}_d) - 2) + (d-1)(q^3+1),$$



whence

$$\mathfrak{g}(\mathcal{X}_d) = \frac{1}{2} \left( \frac{(q^3 + 1)(q^2 - d - 1)}{d} + 2 \right).$$

In particular,  $\mathfrak{g}(\mathcal{X}_d)$  is even. Furthermore, since  $C_d$  is a normal subgroup of  $\text{Aut}(\mathcal{X})$ ,  $\text{Aut}(\mathcal{X})/C_d$  is a subgroup  $G_d$  of  $\text{Aut}(\mathcal{X}_d)$  such that

$$|G_d| = \frac{q^3(q^3 + 1)(q^2 - 1)(q^2 - q + 1)}{d}.$$

Comparing  $|G_d|$  with  $\mathfrak{g}(\mathcal{X}_d)$  shows that if  $d \geq 450$  then  $|\text{Aut}(\mathcal{X}_d)| \geq |G_d| > 900\mathfrak{g}(\mathcal{X}_d)^2$ .

If  $q \not\equiv -1 \pmod{3}$  then both  $(PSU(3, q) \times C_d)/C_d \cong PSU(3, q)$  and  $C_{q^2-q+1}/C_d \cong C_{(q^2-q+1)/d}$  are subgroups of  $G_d$ , and their intersection is trivial. Therefore, they generate a group isomorphic to  $PSU(3, q) \times C_{(q^2-q+1)/d}$  whose order is equal to that of  $G_d$ . Thus  $G_d \cong PSU(3, q) \times C_{(q^2-q+1)/d}$ . This gives an example, not isomorphic to the Hermitian curve, for the case  $p(G) \cong PSU(3, q)$  with  $q \equiv 1 \pmod{3}$  in Theorem 1.2.

If  $q \equiv -1 \pmod{3}$ , take the index 3 subgroup  $G \cong SU(3, q) \times C_{(q^2-q+1)/3}$  together with a subgroup  $C_d$  of  $C_{(q^2-q+1)/3}$ . Then  $d$  is not divisible by 3 and we may replace  $G_d = \text{Aut}(\mathcal{X})/C_d$  with  $G/C_d$  in the above argument. This time we obtain  $G/C_d \cong SU(3, q) \times C_{(q^2-q+1)/3d}$  which gives an example for the case  $p(G) \cong SU(3, q)$  with  $q \equiv -1 \pmod{3}$  in Theorem 1.2.

## 10. THE STRUCTURE OF $G$ IN THEOREM 1.2

**Theorem 10.1.** *With hypotheses and notation as in Theorem 1.2,  $Z(G)$  is a cyclic group, and either  $G = H \times O(G)$  and one of the following cases occurs*

- (I)  $H \cong PSL(2, q)$ ,  $PGL(2, q)$ , and  $O(G) = Z(G)$ ;
- (IIa)  $H \cong PSU(3, q)$ ,  $q \equiv 1 \pmod{4}$ , and  $O(G) = Z(G)$ ;
- (IIb)  $H \cong PGU(3, q)$ ,  $q \equiv 5 \pmod{12}$ , and  $O(G) = Z(G)$  with  $|Z(G)| \not\equiv 0 \pmod{3}$ ;
- (III)  $H \cong SL(2, q)$ ,  $SU^\pm(2, q)$  with  $q \equiv 1 \pmod{4}$ , and  $q = p^k \geq 5$ ,  $[Z(G) : O(G)] = 2$ ;

or  $p(G) \cong PSU(3, q)$  and

- (IIc)  $G \cong (PSU(3, q) \rtimes U) \times N$ ,  $q \equiv 5, 29 \pmod{36}$ , and  $O(G) = Z(G) = U \times N$  with  $|U| = 3^h \geq 9$ ;

or  $G$  has a normal subgroup  $M$  of index either 1 or 3 where

- (IV)  $M \cong SU(3, q) \times N$  and  $[Z(G) : N] = 3$ ,  $|N| \not\equiv 0 \pmod{3}$ ;
- (V)  $M \cong (SU(3, q) \circ U) \times N$ , and  $[Z(G) : N] = 3^h \geq 9$ ,  $|N| \not\equiv 0 \pmod{3}$ ,  $Z(G) = U \times N$ .

*Proof.* If  $p(G) \cong PSL(2, q)$  then  $G/Z(G) \cong PSL(2, q)$  or  $G/Z(G) \cong PGL(2, q)$ . In the former case, (I) of Theorem 10.1 holds and we may assume that the latter case occurs. Since  $[PGL(2, q) : PSL(2, q)] = 2$  and  $|Z(G)|$  is odd, the Sylow 2-subgroups of  $p(G) \times Z(G)$  are subgroups of index 2 in the Sylow 2-subgroups of  $G$ . Therefore, there exists  $m \in G$  of order a power of 2 such that  $m \notin p(G)$ . The subgroup  $M$  generated by  $p(G)$  together with  $m$  has order  $2|p(G)|$ . Also,  $M \cap Z(G) = \{1\}$ . In fact, since each element of  $M$  is a product  $tm$  with  $t \in p(G)$ , the hypothesis  $tm \in Z(G)$  would yield  $m \in p(G) \times Z(G)$ , a contradiction by  $2 \nmid |Z(G)|$ . Therefore  $MZ(G) = M \times Z(G)$ . Hence  $M \times Z(G)$  has order  $2|p(G)||Z(G)|$  equal to  $|PGL(2, q)||Z(G)|$  which is the order of  $G$ . Thus  $G = M \times Z(G)$ , and  $M \cong G/Z(G) \cong PGL(2, q)$  shows that (I) of Theorem 10.1 holds for case  $G/Z(G) \cong PGL(2, q)$ .

If  $p(G) \cong PSU(3, q)$  with  $q \equiv 1 \pmod{4}$ , then  $G/Z(G) \cong PSU(3, q)$  or  $G/Z(G) \cong PGU(3, q)$  with  $q \equiv 5 \pmod{12}$ . In the former case, (IIa) of Theorem 10.1 holds and we may assume that the latter case occurs. From  $[PGU(3, q) : PSU(3, q)] = 3$ , the Sylow 3-subgroup of  $G_P$  for a point  $P \in \Omega$  is larger than that of  $p(G)$ . Therefore, there exists  $m \in G$  of order a power of 3 which is not in  $p(G)$  but fixes a point  $P \in \Omega$ . The subgroup  $M$  generated by  $p(G)$  together with  $m$  has order  $3|p(G)|$ . Two cases arise according as  $|Z(G)|$  is prime to 3 or divisible by 3.

In the former case, the argument used for  $G/Z(G) = PGL(2, q)$  still works showing that  $M \cap Z(G) = \{1\}$ . From this,  $G = M \times Z(G)$  with  $M \cong PGU(3, q)$  whence (IIb) of Theorem 10.1 follows.



In the latter case,  $Z(G) = T \times N$  where  $T$  is a (cyclic) Sylow 3-subgroup of  $Z(G)$ . Then  $H = p(G) \times T$  is a normal subgroup of  $G$ . Furthermore,  $H \cap N = \{1\}$ . In fact, otherwise,  $H \cap N$  would contain a nontrivial element of order prime to 3. Such an element is necessarily contained in  $p(G)$ , whereas  $p(G) \cap Z(G) = \{1\}$ , a contradiction. If  $q + 1 \equiv 0 \pmod{9}$  then  $p(G)$  has an element of order 3 that fixes  $P$ . Such an element is not contained in  $T$  by  $p(G) \cap Z(G) = \{1\}$ . Hence,  $G_P$  contains more than one subgroups of order 3. On the other hand the Sylow 3-subgroup of  $G_P$  is cyclic, a contradiction. Therefore,  $q + 1 \equiv 3, 6 \pmod{9}$ . Then no element of  $p(G)$  of order 3 fixes a point, and the Sylow 3-subgroup  $U$  of  $G$  has order  $3|T|$  where  $p(G) \cap U = \{1\}$ . From this  $|p(G)||U||N| = |G|$ . Thus  $G = (p(G) \rtimes U) \times N$  whence (IIc) of Theorem 10.1 follows.

If  $p(G) \cong SL(2, q)$ , two possibilities occur according as  $G/O(G) \cong SL(2, q)$  or  $G/O(G) \cong SU^\pm(2, q)$ . In the former case, (III) of Theorem 10.1 follows for  $G \cong SL(2, q) \times O(G)$ . In the latter case, since  $[SU^\pm(2, q) : SL(2, q)] = 2$ , the Sylow 2-subgroups of  $G$  are larger than those of  $p(G) \times Z(G)$ , and the above argument for  $PGL(2, q)$  also works for this case. Therefore (III) Theorem 10.1 holds for the case  $G/Z(G) \cong SU^\pm(2, q)$ ,  $q \equiv 1 \pmod{4}$ .

If  $p(G) \cong SU(3, q)$  then two cases arise according as  $|Z(G)| \equiv 3, 6 \pmod{9}$  or  $|Z(G)| \equiv 0 \pmod{9}$ . In the former case,  $Z(G)$  has a prime to 3 subgroup  $N$  of index 3, and  $p(G) \times N$  is a normal subgroup of  $G$ . If  $G/Z(G) \cong PSU(3, q)$  then  $G = p(G) \times N$ , otherwise  $G/Z(G) \cong PGU(3, q)$  and  $p(G) \times N$  is a (normal) subgroup of  $G$  of index 3. In the latter case, write  $Z(G) = U \times N$  where  $U$  is a subgroup of order  $3^h \geq 9$  and  $N$  is a prime to 3 subgroup of  $G$ . Here  $p(G) \cap U$  is a subgroup of order 3 and  $p(G)U/U$  is a central non-split extension. More precisely, it is the central product  $p(G) \circ U$ . Also,  $p(G) \times N$  is a normal subgroup of  $G$ . If  $G/Z(G) \cong PSU(3, q)$  then  $G = (p(G) \circ U) \times N$ , otherwise  $G/Z(G) \cong PGU(3, q)$  and  $(p(G) \circ U) \times N$  is a (normal) subgroup of  $G$  of index 3.  $\square$

**Remark 10.2.** No examples for cases II(c) and (V) are known.

## REFERENCES

- [1] S. Abhyankar, Coverings of algebraic curves, *Amer. J. Math.*, **79** (1957), 825-856.
- [2] A. Adler, The Mathieu group  $M(11)$  and the modular curve  $X(11)$ , *Proc. London Math. Soc.* **74** (1997), 1-28.
- [3] L. Alperin, R. Brauer and D. Gorenstein, Finite simple groups of 2-rank two, *Scripta Math.* **29** (1973), 191-214.
- [4] J.L. Alperin, R. Brauer and D. Gorenstein, Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, *Trans. Amer. Math. Soc.* **151** (1970), 1-261.
- [5] N. Arakelian and G. Korchmáros, A characterization of the Artin-Mumford curve, *J. Number Theory* **154** (2015), 278-291.
- [6] F.M. Bleher, T. Chinburg, B. Poonen and P. Symonds, Automorphisms of HarbaterKatzGabber curves, arXiv:1509.02139.
- [7] I.I. Bouw, The  $p$ -rank of ramified covers, *Compositio Math.* **126** (2001), 209-322.
- [8] R. Brauer and M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group, *Proceedings of the National Academy of Sciences of the United States of America* **45** (1959), 1757-1759.
- [9] M. Conder, Maximal automorphism groups of symmetric Riemann surfaces with small genus, *J. Algebra* **114** (1988), 16-28.
- [10] S. Fanali and M. Giulietti, Quotient curves of the GK curve, *Adv. Geom.* **12** (2012), 239268.
- [11] M. Giulietti and G. Korchmáros, A new family of maximal curves, *Math. Ann.* (2009) **343**, 229-245.
- [12] G. Cornelissen, F. Kato and A. Kontogeorgis, Discontinuous groups in positive characteristic and automorphisms of Mumford curves, *Math. Ann.* **320** (2001), 55-85.
- [13] M. Giulietti and G. Korchmáros, Large 2-groups of automorphisms of curves with positive 2-rank, *J. Algebra*, **427** (2015), 264-294.
- [14] M. Giulietti and G. Korchmáros, Algebraic curves with a large non-tame automorphism group fixing no point, *Trans. Amer. Math. Soc.* **362** (2010), 5983-6001.
- [15] M. Giulietti and G. Korchmáros, Automorphism groups of algebraic curves with  $p$ -rank zero, *J. London Math. Soc.*, (2) **81** (2010) 277-296.
- [16] D. Gorenstein and K. Harada, *Finite Groups Whose 2-Subgroups Are Generated by at Most 4 Elements*, Memoirs of the American Mathematical Society, No. **147**, American Mathematical Society, Providence, R.I., 1974. vii+464 pp.
- [17] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Mathematical Surveys and Monographs*, 40.1. American Mathematical Society, Providence, RI, 1994. xiv+165 pp.

- [18] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups. Number 6. Part IV. The special odd case* Mathematical Surveys and Monographs, 40.6. American Mathematical Society, Providence, RI, 2005. xii+529 pp.
- [19] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I. *J. Algebra* **2** (1965), 85–151.
- [20] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. II. *J. Algebra* **2** (1965), 218–270.
- [21] R. L. Griess, Jr., Schur multipliers of finite simple groups of Lie type, *Trans. Amer. Math. Soc.*, **183** (1973), 355–421.
- [22] J.P. Hansen and J.P. Pedersen, Automorphism group of Ree type, Deligne-Lusztig curves and function fields, *J. Reine Angew. Math.* **440** (1993), 99–109.
- [23] D. Harbater, Abhyankar’s conjecture on Galois groups over curves, *Invent. Math.*, **117** (1994), 1–25.
- [24] D. Harbater, A. Obus, R. Pries, and K. Stevenson, Abhyankar’s conjectures in Galois theory: current status and future directions, arXiv:1408.0859 [math.AG].
- [25] H.W. Henn, Funktionenkörper mit großer Automorphismengruppe, *J. Reine Angew. Math.* **302** (1978), 96–115.
- [26] J.W.P. Hirschfeld, G. Korchmáros and F. Torres *Algebraic Curves Over a Finite Field*, Princeton Univ. Press, Princeton and Oxford, 2008, xx+696 pp.
- [27] C. Hering, A theorem on group space, *Hokkaido Math. J.* **8** (1979), 115–120.
- [28] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967, xii+793 pp.
- [29] V. Landazuri and G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.
- [30] L.M. Isaacs, *Character theory of finite groups*, Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. Dover Publications, Inc., New York, 1994. xii+303 pp.
- [31] H.H. Mitchell, Howard H. Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.* **12** (1911), 207–242.
- [32] S. Nakajima,  $p$ -ranks and automorphism groups of algebraic curves, *Trans. Amer. Math. Soc.* **303** (1987), 595–607.
- [33] M.E. O’Nan, On unitary collineation group, *J. Algebra* **22** (1972), 211–218.
- [34] R.J. Pries, Wildly ramified covers with large genus *J. Number Theory* **119** (2006), 194–209.
- [35] R. Pries and K. Stevenson, A survey of Galois theory of curves in characteristic  $p$ , WIN–women in numbers, 169–191, Fields Inst. Commun., **60**, Amer. Math. Soc., Providence, RI, 2011.
- [36] C.S. Rajan, Automorphisms of  $X(11)$  over characteristic 3 and the Mathieu group  $M(11)$ , *Ramanujan Math. Soc.* **13**, (1998) 63–72.
- [37] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik, *Math. Z.* **117** (1970), 157–163.
- [38] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, *Arch. Math.* **24** (1973), 527–544.
- [39] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. viii+241 pp.
- [40] I.R. Shafarevich, On  $p$ -extensions, *Amer. Math. Soc. Transl.* **4** (1954), 59–71.
- [41] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus 2 function fields, in *Algebra, arithmetic and geometry with applications* (West Lafayette, IN, 2000), 703–723, Springer, Berlin, 2004.
- [42] F. Sullivan,  $p$ -torsion in the class group of curves with many automorphisms, *Arch. Math.* **26** (1975), 253–261.
- [43] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, *Arch. Math.* **24** (1973), 615–631.
- [44] J.G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437.
- [45] R.C. Valentini and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, *J. Reine Angew. Math.* **318** (1980), 156–177.
- [46] J.H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. of Math.* **89** (1969), 405–514.
- [47] R.A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, **251**, Springer-Verlag London, Ltd., London, 2009. xvi+298 pp.

*Authors’ addresses:*

Massimo GIULIETTI  
 Dipartimento di Matematica e Informatica  
 Università degli Studi di Perugia  
 Via Vanvitelli, 1

06123 Perugia (Italy).

E-mail: `massimo.giulietti@unipg.it`

Gábor KORCHMÁROS

Dipartimento di Matematica

Università della Basilicata

Contrada Macchia Romana

85100 Potenza (Italy).

E-mail: `gabor.korchmaros@unibas.it`